

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE



Japanese Patent Application of

S. SAWADA et al

Serial No. 09/893,004

Filed: June 28, 2001

ATTN: Manager,
Applications BranchFor: COMMUNICATION APPARATUS FOR ROUTING OR
DISCARDING A PACKET SENT FROM A USER TERMINALTRANSMITTAL OF LATE DECLARATION AND
CERTIFIED PRIORITY DOCUMENTCommissioner for Patents
Washington, D.C. 20231

September 20, 2001

Sir:

Responsive to the NOTICE TO FILE MISSING PARTS OF
APPLICATION - FILING DATE GRANTED mailed August 21, 2001, Applicants
submit herewith the executed Declaration and Power of Attorney,
along with the required surcharge as set forth in 37 CFR 1.16(e).

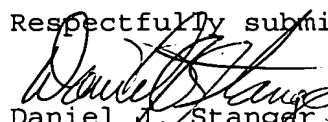
Our check in the amount of \$130.00 is attached.

As required, a copy of the NOTICE (PART 2) of August 21, 2001
is enclosed herewith.

Also submitted is a certified priority document of
corresponding Japanese Patent Application No. 2000-195706 filed June
29, 2000 for the purpose of claiming foreign priority under 35
U.S.C. § 119. An indication that this document has been safely
received would be appreciated.

Please charge any additional fees which may be required, or
credit any overpayment to our Deposit Account No. 50-1417.

Respectfully submitted,


Daniel J. Stanger
Registration No. 32,846
Attorney for Applicant(s)

MATTINGLY, STANGER & MALUR
1800 Diagonal Rd., Suite 370
Alexandria, Virginia 22314
(703) 684-1120
Date: September 20, 2001



340000934 US/

#3

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application:

2000年 6月29日

出願番号

Application Number:

特願2000-195706

出願人

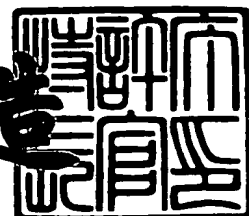
Applicant(s):

株式会社日立製作所

2001年 4月20日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造



出証番号 出証特2001-3032428

【書類名】 特許願

【整理番号】 P0264JP

【提出日】 平成12年 6月29日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 29/02

【発明者】

【住所又は居所】 神奈川県秦野市堀山下1番地 株式会社日立製作所 エ
ンタープライズサーバ事業部内

【氏名】 澤田 素直

【発明者】

【住所又は居所】 神奈川県秦野市堀山下1番地 株式会社日立製作所 エ
ンタープライズサーバ事業部内

【氏名】 綿貫 達哉

【発明者】

【住所又は居所】 神奈川県秦野市堀山下1番地 株式会社日立製作所 エ
ンタープライズサーバ事業部内

【氏名】 野崎 信司

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社日立製作所

【代理人】

【識別番号】 100107010

【弁理士】

【氏名又は名称】 橋爪 健

【手数料の表示】

【予納台帳番号】 054885

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

特 2 0 0 0 - 1 9 5 7 0 6

【物件名】	図面	1
【物件名】	要約書	1
【ブルーフの要否】	要	

【書類名】 明細書

【発明の名称】 ネットワーク間接続装置及びネットワークシステム

【特許請求の範囲】

【請求項 1】

ネットワークを介して配されたユーザ端末、認証サーバ及びファイルサーバ間でパケットを送受信するネットワークシステムにおけるネットワーク間接続装置であって、

複数のネットワークインターフェースと、

パケットを送信すべき前記ネットワークインターフェースを特定するための情報を含むアドレス学習テーブルと、

前記学習テーブルを参照して、前記ネットワークインターフェースの状態に基づいて、パケットの中継先を選択すると共に、ユーザ端末、認証サーバ及びファイルサーバ間のパケットを中継又は廃棄するパケット中継部と、

特定のネットワークインターフェースの状態を接続状態、非接続状態及び状態なしのいずれかの状態に変更する指示を保持する状態変更指示パケットを、前記パケット中継部を介して認証サーバから受信する状態変更指示パケット処理部と

特定のネットワークインターフェース内にそれぞれ設けられ、前記状態変更指示パケット処理部からの状態変更指示パケットを受信すると共に、該状態変更指示パケットに基づいて、特定のネットワークインターフェースの状態を接続状態、非接続状態及び状態なしのいずれかの状態に変更する状態管理部とを備えたネットワーク間接続装置。

【請求項 2】

前記ネットワークシステムでは、ネットワーク及びルータを介して配されたユーザ端末に動的にアドレスを配布するアドレス割り当てサーバをさらに備え、

受信したパケットの送信元アドレスを登録するフィルタリングテーブルをさらに備え、

前記状態変更指示パケット処理部は、

前記フィルタリングテーブルに登録された特定のアドレスを、前記アドレス学

習テーブルに登録するように指示する状態変更指示パケットを受信した場合、該特定のアドレスをアドレス学習テーブルに登録し、

パケットの宛先アドレスが、アドレス学習テーブルに登録されている場合、パケットを中継し、

パケットの宛先アドレスが、アドレス学習テーブルに未登録であり、かつ、前記フィルタリングテーブルに登録され、パケットの送信元アドレスが、ルータ又は認証サーバである場合、パケットを中継するようにした請求項 1 に記載のネットワーク間接続装置。

【請求項 3】

前記ネットワークインターフェースは、ネットワークが使用可能であるかどうかを検出する回線断検出部をさらに備え、

前記状態管理部は、

前記回線断検出部により回線断が検出された場合、回線断が検出されたネットワークインターフェースの状態を非接続状態に変更し、

前記認証サーバによりユーザ端末が認証を受けた場合、該ユーザ端末に接続されたネットワークインターフェースの状態を接続状態に変更し、

前記パケット中継部は、

非接続状態のネットワークインターフェースからパケットを受信した場合、パケットを、非接続状態又は接続状態のネットワークインターフェースには中継せず、特定のネットワークインターフェースにのみ中継し、

接続状態のネットワークインターフェースからパケットを受信した場合、パケットを、非接続状態のネットワークインターフェースには中継しないようにした請求項 1 又は 2 に記載のネットワーク間接続装置。

【請求項 4】

ネットワークを介して配されたユーザ端末、認証サーバ及びファイルサーバ間でパケットを送受信するネットワークシステムにおけるネットワーク間接続装置であって、

ネットワークに接続するための物理インターフェースと、

パケットの中継先を選択するパケット中継部と、

パケットを中継又は廃棄するための情報を含むフィルタリングテーブルと、前記フィルタリングテーブルの内容に基づいて、パケットを廃棄又は前記パケット中継部に送信するパケット処理部とを有し、前記物理インターフェースとパケット中継部との間に配され、パケットフィルタリングを行うフィルタリング処理部と、

前記フィルタリング処理部に対して、前記認証サーバからのフィルタリング変更指示を送信し、かつ、受信したパケットを全て廃棄するように初期設定された前記フィルタリングテーブル内の情報を、前記認証サーバからの指示に基づいて変更し、前記認証サーバにより認証を受けたユーザ端末のアドレスを送信元アドレスとするパケットを前記ファイルサーバに中継するための情報を、前記フィルタリングテーブルに順次追加するフィルタリング変更指示処理部とを備えたネットワーク間接続装置。

【請求項5】

ネットワークを介して配されたユーザ端末、認証サーバ及びファイルサーバ間でパケットを送受信するネットワークシステムにおけるネットワーク間接続装置であって、

ユーザ端末、認証サーバ及びファイルサーバからのパケットを送受信するネットワークインターフェースと、

認証サーバにより認証を受けたユーザ端末のアドレスを登録するIPアドレス登録表と、

前記IPアドレス登録表に登録されたアドレスを送信元アドレスとするパケットを中継し、IPアドレス登録表に未登録のアドレスを送信元アドレスとするパケットはカプセル化した後、特定のアドレス宛に送信するパケット中継部とを備えたネットワーク間接続装置。

【請求項6】

請求項1乃至5のいずれかに記載のネットワーク間接続装置と、

前記ネットワーク間接続装置にネットワークを介して接続されたユーザ端末と、

ファイルサーバと、

前記ユーザ端末に対して、前記ファイルサーバへのアクセスを許可するための
認証を行う認証サーバと
を備えたネットワークシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ネットワーク間接続装置及びネットワークシステムに係り、特に、
LANスイッチやルータ等を用いたネットワークの不正使用を防止するネットワ
ーク間接続装置及びネットワークシステムに関する。

【0002】

【従来の技術】

近年、各種ネットワークが保持する情報に対する信用を確保するために、ネッ
トワークの利用を制限する情報セキュリティ技術の必要性が認識されている。一
方、ネットワークの利便性を考えて、例えば、IEEE (Institute of Electri
cal and Electronics Engineers, Inc.) で規定されているCSMA/CD (Car
rier Sense Multiple Access with Collision Detection) 型の802.3ネッ
トワークに代表されるLAN (Local Area Network) では、ネットワークに端末
を接続しさえすれば使用できるようになっている。

【0003】

また、IETF (Internet Engineering Task Force) で標準化されたDHC
P (Dynamic Host Configuration Protocol) を用いれば、新たに接続された端
末に対して自動的にアドレスを割り当てることができる。これらのネットワーク
とノート型パソコンのような可搬型の端末により、自由な場所で必要な時にネッ
トワークを利用できる情報コンセントシステムが登場している（例えば、“生徒
のための、生徒による、生徒のネットワーク作り物語”，pp.66, UNIX USER, vo
l.8, No.4, APR.1 1999）。

【0004】

【発明が解決しようとする課題】

しかしながら、ネットワークの利用が容易になることで、ネットワークの使用

許可を得ていない不正な利用者（不正ユーザ）であっても、ネットワークに端末を接続しさえすればネットワークを利用できてしまう場合が想定される。このため、ネットワークに接続されたファイルサーバなどの資源は、不正ユーザからの不正なアクセスにさらされるというセキュリティ上の不都合が生じてしまう。

【0005】

こうした不正なアクセスの防止に用いられる技術として、ルータ等のネットワーク間接続装置によるパケットフィルタリングが知られている。しかし、パケットフィルタリングの条件は予め設定しておかなければならず、上述の情報コンセントシステムのように、任意の位置で動的に配布されたアドレスを用いているネットワークでは、予めパケットフィルタリングの条件を決めておくことは困難である。

【0006】

本発明は、以上の点に鑑み、不正な利用者がネットワークを不正に利用することを防止するネットワーク間接続装置及びネットワークシステムを提供することを目的とする。

また、本発明は、ユーザが自由な位置で、その度に違うアドレスでネットワークに接続しても、そのユーザに対して許可されたネットワーク資源にしかアクセスできないネットワーク間接続装置及びネットワークシステムを提供することを目的とする。

【0007】

【課題を解決するための手段】

本発明の第1の解決手段によると、

ネットワークを介して配されたユーザ端末、認証サーバ及びファイルサーバ間でパケットを送受信するネットワークシステムにおけるネットワーク間接続装置であって、

複数のネットワークインターフェースと、

パケットを送信すべき前記ネットワークインターフェースを特定するための情報を含むアドレス学習テーブルと、

前記学習テーブルを参照して、前記ネットワークインターフェースの状態に基

づいて、パケットの中継先を選択すると共に、ユーザ端末、認証サーバ及びファイルサーバ間のパケットを中継又は廃棄するパケット中継部と、

特定のネットワークインターフェースの状態を接続状態、非接続状態及び状態なしのいずれかの状態に変更する指示を保持する状態変更指示パケットを、前記パケット中継部を介して認証サーバから受信する状態変更指示パケット処理部と、

特定のネットワークインターフェース内にそれぞれ設けられ、前記状態変更指示パケット処理部からの状態変更指示パケットを受信すると共に、該状態変更指示パケットに基づいて、特定のネットワークインターフェースの状態を接続状態、非接続状態及び状態なしのいずれかの状態に変更する状態管理部とを備えたネットワーク間接続装置を提供する。

【 0 0 0 8 】

本発明の第 2 の解決手段によると、

ネットワークを介して配されたユーザ端末、認証サーバ及びファイルサーバ間でパケットを送受信するネットワークシステムにおけるネットワーク間接続装置であって、

ネットワークに接続するための物理インターフェースと、

パケットの中継先を選択するパケット中継部と、

パケットを中継又は廃棄するための情報を含むフィルタリングテーブルと、前記フィルタリングテーブルの内容に基づいて、パケットを廃棄又は前記パケット中継部に送信するパケット処理部とを有し、前記物理インターフェースとパケット中継部との間に配され、パケットフィルタリングを行うフィルタリング処理部と、

前記フィルタリング処理部に対して、前記認証サーバからのフィルタリング変更指示を送信し、かつ、受信したパケットを全て廃棄するように初期設定された前記フィルタリングテーブル内の情報を、前記認証サーバからの指示に基づいて変更し、前記認証サーバにより認証を受けたユーザ端末のアドレスを送信元アドレスとするパケットを前記ファイルサーバに中継するための情報を、前記フィルタリングテーブルに順次追加するフィルタリング変更指示処理部と

を備えたネットワーク間接続装置を提供する。

【 0 0 0 9 】

本発明の第 3 の解決手段によると、

ネットワークを介して配されたユーザ端末、認証サーバ及びファイルサーバ間でパケットを送受信するネットワークシステムにおけるネットワーク間接続装置であって、

ユーザ端末、認証サーバ及びファイルサーバからのパケットを送受信するネットワークインターフェースと、

認証サーバにより認証を受けたユーザ端末のアドレスを登録する IP アドレス登録表と、

前記 IP アドレス登録表に登録されたアドレスを送信元アドレスとするパケットを中継し、IP アドレス登録表に未登録のアドレスを送信元アドレスとするパケットはカプセル化した後、特定のアドレス宛に送信するパケット中継部とを備えたネットワーク間接続装置を提供する。

【 0 0 1 0 】

本発明の第 4 の解決手段によると、

上述に記載のネットワーク間接続装置と、

前記ネットワーク間接続装置にネットワークを介して接続されたユーザ端末と

ファイルサーバと、

前記ユーザ端末に対して、前記ファイルサーバへのアクセスを許可するための認証を行う認証サーバと

を備えたネットワークシステムを提供する。

【 0 0 1 1 】

本発明の特徴のひとつとしては、複数のネットワークインターフェースとパケット中継手段とを有し、各ネットワークインターフェースが、接続状態、非接続状態、状態なしのいずれの状態であるかを保持する状態管理手段を有し、該各ネットワークインターフェースの状態が該パケット中継手段におけるパケットの中継先の選択に影響する。

【 0 0 1 2 】

本発明の他の特徴としては、状態変更指示パケット処理手段を有し、状態変更指示パケットで指示された前記ネットワークインターフェースの状態を該状態変更指示パケットで指示された状態に変更することができる。

【 0 0 1 3 】

本発明の他の特徴としては、前記各ネットワークインターフェースは回線断検出手段を有し、該回線断検出手段により回線断が検出されると該ネットワークインターフェースの状態を非接続状態に変更することができる。

【 0 0 1 4 】

本発明の他の特徴としては、初期化時に各ネットワークインターフェースの状態が非接続状態に初期化されるようにしてもよい。

【 0 0 1 5 】

本発明の他の特徴としては、非接続状態の該ネットワークインターフェースから受信したパケットを特定の該ネットワークインターフェースのみに中継することができる。

【 0 0 1 6 】

本発明の他の特徴としては、非接続状態の該ネットワークインターフェースから受信したパケットを、非接続状態あるいは接続状態の該ネットワークインターフェースに中継しないようにしてもよい。

【 0 0 1 7 】

本発明の他の特徴としては、接続状態の該ネットワークインターフェースから受信したパケットを非接続状態の該ネットワークインターフェースに中継しないようにしてもよい。

【 0 0 1 8 】

本発明の他の特徴としては、上述のネットワーク間接続装置を適用したネットワークシステムであって、認証を行ったユーザの使用する端末の接続されたネットワークインターフェースの状態を接続状態に変更するようにしてもよい。

【 0 0 1 9 】

本発明の他の特徴としては、上述のネットワーク間接続装置を適用したネット

ワークシステムであって、複数のネットワークインターフェース、パケット中継手段、フィルタリングテーブル、該フィルタリングテーブルの内容によってパケットフィルタリングを行うパケットフィルタリング手段、及び該フィルタリングテーブルの内容を外部からの指示により変更するフィルタリング変更指示処理手段を有し、初期状態では該フィルタリングテーブルの内容を全ての受信パケットを廃棄する用に設定されたネットワーク間接続装置に対し、外部からの指示で特定の送信元アドレスを持つパケットの中継を許可する内容を該フィルタリングテーブルに順次追加していくことができる。

【 0 0 2 0 】

本発明の他の特徴としては、上述のネットワーク間接続装置を適用したネットワークシステムであって、順次追加していく内容は、認証を受けたユーザが使用する端末のアドレスを送信元アドレスとして持つパケットの中継許可であるようにしてもよい。

【 0 0 2 1 】

本発明の他の特徴としては、複数のネットワークインターフェース、パケット中継手段、フィルタリングテーブル、アドレス学習テーブル及び状態変更指示パケット処理手段を有し、受信したパケットの送信元アドレスを該フィルタリングテーブルに登録し、該フィルタリングテーブル内に登録された特定のアドレスを該アドレス学習テーブルに登録するよう指示する状態変更指示パケットを受信した場合に、該状態変更指示パケット処理手段が該フィルタリングテーブルに登録された特定のアドレスを該アドレス学習テーブルに登録するようにしてもよい。

【 0 0 2 2 】

本発明の他の特徴としては、前記学習テーブルに登録されたアドレス宛のパケットを中継し、該学習テーブルに登録されてなく、かつ、前記フィルタリングテーブルに登録されているアドレス宛のパケットは、特定の送信元アドレスを有している場合にのみ中継することができる。

【 0 0 2 3 】

本発明の他の特徴としては、上述のネットワーク間接続装置を適用したネットワークシステムであって、認証を受けたユーザの使用する端末のアドレスを前記

学習テーブルに登録することを指示することができる。

【 0 0 2 4 】

本発明の他の特徴としては、複数のネットワークインターフェース、パケット中継手段、及びアドレス登録表を有し、該アドレス登録表に登録されたアドレスを送信元アドレスとするパケットは、中継し、該アドレス登録表に登録されていないアドレスを送信元アドレスとするパケットは、カプセル化した後、特定のアドレス宛に送信するようにしてもよい。

【 0 0 2 5 】

本発明の他の特徴としては、上述のネットワーク間接続装置を適用したネットワークシステムであって、前記アドレス登録表に登録されていないアドレスを送信元アドレスとするパケットをカプセル化して送信する特定のアドレスが、ユーザの認証を行う装置のアドレスであるようにしてもよい。

【 0 0 2 6 】

本発明の他の特徴としては、上述のネットワーク間接続装置を適用したネットワークシステムであって、認証を受けたユーザの使用する端末のアドレスを前記アドレス登録表に登録するようにしてもよい。

【 0 0 2 7 】

本発明の他の特徴としては、ネットワーク間接続装置の各ネットワークインターフェースで「非接続状態」かどうかを管理し、「非接続状態」である場合、通信を遮断するようにしてもよい。

【 0 0 2 8 】

本発明の他の特徴としては、ネットワークから端末が離脱した場合、この離脱を検出したネットワークインターフェースでは、自動的に「非接続状態」に切り替わるようにしてもよい。

【 0 0 2 9 】

本発明の他の特徴としては、ユーザに対して割り当てられたアドレスを把握し、この把握したアドレスに基づいてパケットフィルタリングの設定を行うようにしてもよい。

【 0 0 3 0 】

【発明の実施の形態】

以下、図面を用いて本発明の実施の形態を詳細に説明する。

(第1の実施の形態)

図1は、本発明に関するネットワーク間接続装置の第1の実施の形態の構成図である。

LANスイッチ100は、例えば、パケット中継手段101、複数のネットワークインターフェース102～107、アドレス学習テーブル108及び状態変更指示パケット処理手段109を備える。ネットワークインターフェース102～107には、それぞれを一意に識別するために名前(図ではA～F)が割り当てられている。なお、名前は、一意に識別できれば番号等を用いてもよい。

【0031】

これらのネットワークインターフェース102～107は、それぞれ異なるネットワークと接続されており、パケットの送受信を行う。なお、本実施の形態では、ネットワークとしてIEEEで規定されているCSMA/CD型の802.3ネットワークを、ツイストペア線で接続することを想定しているが、本発明は、その他のネットワーク(例えば無線ネットワーク)にも適用可能である。

【0032】

パケット中継手段101は、全てのネットワークインターフェース102～107と接続されており、OSI(Open System Interconnection)モデルのデータリンク層でパケット中継を行う。アドレス学習テーブル108には、パケット中継手段101がパケットを送信すべきネットワークインターフェースを判断するために必要な情報が格納されている。

【0033】

図3は、アドレス学習テーブル108の構成図(1)である。

アドレス学習テーブル108の各エントリは、アドレスフィールド301と送信ポートフィールド302を含む。アドレスフィールド301には、物理アドレス(以下、MACアドレスと表記する)が、送信ポートフィールド302には、ネットワークインターフェースの名前が、それぞれ格納される。ここで、アドレス学習テーブル108の各エントリは、パケットを中継する際、パケットの宛先

アドレスがアドレスフィールド 3 0 1 に一致した場合、同じエントリの送信ポートフィールド 3 0 2 で示されるネットワークインターフェースから、パケットを送信することを表している。なお、送信ポートフィールド 3 0 2 には、複数のネットワークインターフェースを登録することができる。例えば、特殊なケースとして、LAN スイッチ 1 0 0 自体のアドレスをアドレスフィールド 3 0 1 に登録し、送信ポートフィールド 3 0 2 を「X」とした場合、このエントリは、該当するパケットを、LAN スイッチ 1 0 0 宛のパケットとして処理することを示している。

【 0 0 3 4 】

状態変更指示パケット処理手段 1 0 9 は、LAN スイッチ 1 0 0 に接続されたいずれかのネットワークを介して、外部（例えば、後述する認証サーバ 4 0 1）より LAN スイッチ 1 0 0 宛に送られた状態変更指示パケットを、パケット中継手段 1 0 1 を介して受信すると共に、この状態変更指示パケットの内容を適当なネットワークインターフェース 1 0 2 ～ 1 0 7 に通知する。状態変更指示パケットは、特定のネットワークインターフェースの状態を特定の状態に変更する指示を情報として保持している。なお、プロトコルとしては、例えば、SNMP（Simple Network Management Protocol）を使用するが、他にも `telnet`（telecommunications network protocol）や HTTP（Hyper Text Transfer Protocol）などのプロトコルを利用してもよい。また、本実施の形態では、ネットワーク間接続装置として LAN スイッチ 1 0 0 を使用しているが、ルータ等その他のネットワーク間接続装置に対しても、本発明は適用可能である。

【 0 0 3 5 】

図 2 は、ネットワークインターフェース 1 0 2 ～ 1 0 7 の構成図である。

ネットワークインターフェース 1 0 2 ～ 1 0 7 は、例えば、ネットワークに接続するための物理インターフェース 2 0 1、ネットワークが使用可能であるかどうかを検出する回線断検出手段 2 0 2 及びネットワークインターフェースの状態を管理する状態管理手段 2 0 3 を備え、物理インターフェース 2 0 1 と状態管理手段 2 0 3 は、パケット中継手段 1 0 1 にそれぞれ接続されている。

【 0 0 3 6 】

回線断検出手段 2 0 2 は、ネットワークの回線（ケーブル）が接続されているかどうか、又は回線を介して接続されている端末が使用可能な状態（電源投入状態）であるかどうかを電氣的に検出すると共に、検出された回線断を状態管理手段 2 0 3 に通知する。また、本実施の形態では、回線断の検出にあたって、物理インターフェース 2 0 1 から通知されるリンクダウン状態が 1 0 0 m s 以上続いた場合に、回線断と判定している。なお、回線として光ファイバを用いている場合は光信号の有無が、無線ならば電波の有無がそれぞれ同様に回線断の検出に使用できる。

【 0 0 3 7 】

状態管理手段 2 0 3 は、ネットワークインターフェースの状態が「接続状態」、「非接続状態」及び「状態なし」のいずれであるかを管理する。ユーザ（スイッチ管理者）は、各ネットワークインターフェース 1 0 2 ～ 1 0 7 の状態管理手段 2 0 3 に対して、常に「接続状態」または「状態なし」になるように予め設定することができる。各ネットワークインターフェース 1 0 2 ～ 1 0 7 の状態は、ユーザによる設定があればそのように、設定がなければ「非接続状態」となる。また、回線断検出手段 2 0 2 により回線断が状態管理手段 2 0 3 に通知されると、ユーザによる事前の設定がない場合、該当するネットワークインターフェースの状態は「非接続状態」になる。さらに、状態変更指示パケット処理手段 1 0 9 による指示があった場合、その指示に基づいて上述の三つの状態のいずれかに変更される。

【 0 0 3 8 】

つぎに、図 4 のネットワークを例に、本発明に関するネットワーク間接続装置を用いたネットワークの動作を説明する。

図 4 は、本発明に関する LAN 1 0 0 を用いたネットワークの構成図である。

このネットワークは、例えば、LAN スイッチ 1 0 0 （アドレス 2 2 : 2 2 : 0 0 : F F : F F : F F）と、LAN スイッチ 1 0 0 のネットワークインターフェース A 1 0 2 に接続された認証サーバ 4 0 1 （アドレス 2 2 : 2 2 : 0 0 : 1 1 : 1 1 : 1 1）と、ネットワークインターフェース B 1 0 3 に接続されたファイルサーバ 4 0 2 （アドレス 2 2 : 2 2 : 0 0 : 2 2 : 2 2 : 2 2）と、ネット

ワークインターフェースC104～F107にそれぞれ接続され、ユーザが端末を自由に接続してネットワークを利用できる、いわゆる情報コンセント409と、情報コンセント409を介してネットワークインターフェースC104に接続されたユーザ端末403（アドレス22:22:FF:00:00:01）とを備える。

【0039】

認証サーバ401は、ユーザがネットワークの使用を許可されているかどうかを判断し、その結果をLANスイッチ100に通知する。本実施の形態では、ユーザの認証を、ユーザIDとパスワードを用いて行う。また、LANスイッチ100の各ネットワークインターフェースC102～F107の設定は、ネットワークインターフェースB103は常に「接続状態」、ネットワークインターフェースA102は「状態なし」にそれぞれ設定し、ネットワークインターフェースC104～F107は特に設定をしない。したがって、ネットワークインターフェースC104～F107は、初期化時に「非接続状態」となる（なお、この際、LANスイッチ100の学習テーブル108は、図3に示すようになっている。）。

【0040】

つぎに、このネットワークで、ユーザ端末403（アドレス22:22:FF:00:00:01）がネットワークインターフェースC104につながる情報コンセント409に接続された場合について説明する。

図5は、ユーザ端末403を情報コンセント409に接続した際の通信シーケンス図である。

まず、認証を受けていないユーザ端末403が、ファイルサーバ402にアクセスする場合、ユーザ端末403から、宛先アドレスがファイルサーバ402のアドレス（22:22:00:22:22:22）、かつ、送信元アドレスがユーザ端末403のアドレス（22:22:FF:00:00:01）であるファイルサーバ宛パケット501が送信される。ここで、パケット501を受信したLANスイッチ100の中継処理を説明する。

【0041】

図6は、パケット受信に対するLANスイッチ100の中継処理を示すフローチャートである。

まず、パケット501の送信元アドレス（ユーザ端末403のアドレス22：22：FF：00：00：01）を学習テーブル108に登録する。また、送信ポートフィールド302として登録されるネットワークインターフェースはCとなる。

【0042】

図7は、アドレス学習テーブル108の構成図（2）である。

学習テーブル108のエントリ#4には、上述のように送信元アドレスとして、ユーザ端末403のアドレスが登録され、送信ポートとして、ネットワークインターフェースCがそれぞれ登録される。

【0043】

つぎに、ファイルサーバ402の宛先アドレス（22：22：00：22：22：22）が学習テーブル108に登録済みであるので（処理602）、学習テーブル108の送信ポートフィールド302の内容に基づいて、を送信ポートBを取得すると共に（処理603）、中継処理を行う（処理604）。

【0044】

ここで、処理604について説明する。

図8は、処理604のフローチャートである。

まず、送信ポート（この場合ネットワークインターフェースB103）と受信ポート（この場合ネットワークインターフェースC104）とが同一かどうかを判定する（処理801）。ここでは、送信ポートと受信ポートは異なるポートであるので、後述する中継テーブル901に基づいて、パケット中継を行う（処理802）。

【0045】

図9は、中継テーブル901の構成図である。

中継テーブル901は、受信ポートの状態と送信ポートの状態に基づいて、パケットの中継／廃棄を判定するためのテーブルである。ここでは、ユーザ端末403から送信されたパケット501を受信するLANスイッチ100の受信ポー

ト（ネットワークインターフェースC104）は「非接続状態」であり、送信ポート（ネットワークインターフェースB103）は「接続状態」であるので、中継テーブル901により「廃棄」の結果が得られる。このため、パケット501は廃棄される。これにより、認証を受けていないユーザ端末403からのファイルサーバ402へのアクセスは回避されたことになる。

【0046】

さらに、続いて、ユーザ端末403が、認証サーバ401に認証サーバ宛パケット502を送信する場合について説明する。ユーザ端末403が、宛先アドレスが認証サーバ401のアドレス（22：22：00：11：11：11）であり、かつ、送信元アドレスがユーザ端末403のアドレス（22：22：FF：00：00：01）であるパケット502を送信する。このパケット502を受信したLANスイッチ100は、上述した図6に従い中継処理を行う。

【0047】

まず、学習テーブル108には、先のパケット501受信時、アドレス（22：22：FF：00：00：01）が既に登録されているので、処理601を通過する。つぎに、宛先アドレス（22：22：00：11：11：11）が学習テーブル108に登録済みであるので（処理602）、送信ポートフィールド302の内容に基づいて、送信ポート（A）から中継処理を行う（処理604）。

【0048】

ここで、再び、図8及び9を用いて処理604について説明する。

まず、送信ポート（A）が受信ポート（C）とは異なるので（処理801）、処理802に進む。受信ポートの状態は「非接続状態」、送信ポートの状態は「状態なし」であるので、中継テーブル901より「中継」の結果が得られる。このため、パケット502はネットワークインターフェースA102から認証サーバ401に中継される。

【0049】

さらに、認証サーバ401からユーザ端末403への応答のパケット503は、同様の中継処理により、受信ポートが「状態なし」、送信ポートが「非接続状態」であるので、「中継」となる。つまり、認証サーバ401とユーザ端末40

3との間で双方向の通信が成立することになり、ユーザの認証が行える。

【0050】

認証サーバ401では、例えば、ユーザ端末403から送られてきたユーザID及びパスワード504がネットワークの使用許可を与えられたユーザのものと一致した場合、LANスイッチ100に対して接続許可を通知する。この接続許可の通知には、宛先アドレスがLANスイッチ100のアドレス(22:22:00:FF:FF:FF)である状態変更指示パケット505を送信する。パケット505には、「接続状態への状態変更」とユーザ端末403のアドレス(22:22:FF:00:00:01)が情報として含まれている。

【0051】

状態変更指示パケット505を受信したLANスイッチ100は、学習テーブル108により、宛先アドレスに対応する送信ポートフィールド302が「X」であるので(処理602)、パケット505は、状態変更指示パケット処理手段109に送られる(処理605)。状態変更指示パケット処理手段109は、パケット505に含まれる情報からユーザ端末403のアドレス(22:22:FF:00:00:01)を取得すると共に、このアドレスを学習テーブル108のアドレスフィールド301から検索する。この検索で得られたエントリの送信ポートフィールド302に示されたネットワークインターフェース(この場合はC)に対して、状態を「接続状態」に変更するように指示する。

【0052】

ネットワークインターフェースC104の状態が「接続状態」に変更されることで、ユーザ端末403からファイルサーバ宛パケット506を送信する場合、受信ポートが「接続状態」であり、かつ、送信ポートが「接続状態」であるため、中継テーブル901により「中継」となる。これにより、ユーザ端末403からファイルサーバ402へのアクセスが可能となる。

【0053】

次に、ユーザ端末403が情報コンセント409から離脱した場合のLANスイッチ100の動作を説明する。

ユーザ端末403が情報コンセント409からケーブル(ツイストペア線)を

抜いて接続を解除すると、ネットワークインターフェースC104の物理インターフェース201が回線断の状態になる。その状態で100msが経過すると、回線断検出手段202は、状態管理手段203に回線断を通知する。回線断を通知された状態管理手段203は、ネットワークインターフェースC104の状態を「非接続状態」に変更する。これにより、新たなユーザ端末が同じ情報コンセント409に接続された場合でも、あらためて認証を受けるまではファイルサーバ402にアクセスできなくなる。

【0054】

以上のように、本実施の形態のLANスイッチ100を用いることで、認証前のユーザ端末403からは、ファイルサーバ402へのアクセスが阻止され、認証後はアクセスが可能になり、さらに、ユーザ端末403の離脱後は、再び認証を行うまではファイルサーバ402へのアクセスが阻止されるネットワークシステムを構築することができる。また、本実施の形態では、ユーザ端末403がネットワークインターフェースC104につながる情報コンセント409に接続された場合について説明したが、ネットワークインターフェースC104～F107の動作は同様であり、ユーザ端末403が任意の情報コンセント409に接続されても同様の効果が得られる。

【0055】

また、本実施の形態では、ネットワークインターフェースの状態を、回線断により「非接続状態」に再初期化したが、ユーザが離脱前に認証サーバ401と通信して離脱を通知し、その通知を受けた認証サーバ401は、「非接続状態に状態変更」とユーザ端末403のアドレスとを情報として持つパケットを、LANスイッチ100のアドレス(22:22:00:FF:FF:FF)宛に送り、状態変更指示パケット処理手段109により、ネットワークインターフェースの状態を「非接続状態」に変更することも可能である。これにより、ユーザは、ユーザ端末403と情報コンセント409の接続を切らずに、ネットワークの使用可否を制御できる。

【0056】

(第2の実施の形態)

図 1 0 は、本発明に関するネットワーク間接続装置の第 2 の実施の形態の構成図である。

ルータ 1 0 0 0 は、例えば、複数の物理インターフェース 1 0 0 2 ~ 1 0 0 7、パケット中継手段 1 0 0 1、複数のフィルタリング処理部 1 0 1 2 ~ 1 0 1 7 及びフィルタリング変更指示処理手段 1 0 0 9 を備える。物理インターフェース 1 0 0 2 ~ 1 0 0 7 は、それぞれ異なるネットワークと接続されており、パケットの送受信を行う。パケット中継手段 1 0 0 1 は、I P (Internet Protocol) プロトコルに基づいたパケット中継を行う。なお、本実施の形態では、パケット中継のプロトコルとして I P プロトコルを用いたが、本発明は、例えば、I P v 6 (I P version 6) など、その他のネットワーク層プロトコル、にも適用可能である。また、本実施の形態では、ネットワーク間接続装置としてルータ 1 0 0 0 を使用しているが、L A N スイッチ等その他のネットワーク間接続装置に対しても、本発明は適用可能である。

【0057】

図 1 1 は、フィルタリング処理部 1 0 1 2 ~ 1 0 1 7 の構成図である。

フィルタリング処理部 1 0 1 2 ~ 1 0 1 7 は、フィルタリングテーブル 1 1 0 1、パケット処理部 1 1 0 2 を備える。フィルタリングテーブル 1 1 0 1 には、パケットの中継または廃棄の判断のための情報が格納されている。パケット処理部 1 1 0 2 は、フィルタリングテーブル 1 1 0 1 の情報に基づいて、パケットの廃棄又は、パケット中継手段 1 0 0 1 への送信を行う。パケット中継手段 1 0 0 1 に送られたパケットは、物理インターフェース 1 0 0 2 ~ 1 0 0 7 に送信される。各フィルタリングテーブル 1 1 0 1 は、フィルタリング変更指示処理手段 1 0 0 9 と接続されており、フィルタリング変更指示処理手段 1 0 0 9 からの指示に応じてフィルタリングテーブル 1 1 0 1 の内容を変更することができる。

【0058】

図 1 2 は、フィルタリングテーブル 1 1 0 1 の構成図 (1) である。

フィルタリングテーブル 1 1 0 1 は、パケットの中継または廃棄の判断のための情報を格納しており、各エントリは、宛先アドレス条件 1 2 0 1、送信元アドレス条件 1 2 0 2、中継／廃棄フラグ 1 2 0 3 を含む。宛先アドレス条件 1 2 0

1 及び送信元アドレス条件 1 2 0 2 には、IP アドレスまたは「任意」が登録されている。中継／廃棄フラグ 1 2 0 3 には、宛先アドレスと送信元アドレスがそれぞれ宛先アドレス条件 1 2 0 1 と送信元アドレス条件 1 2 0 2 に一致した受信パケットを中継すべきか又は廃棄すべきかが登録されている。複数のエントリに一致するパケットの場合は、テーブルの先頭に近いエントリが適用される。また、一致するエントリが一つもないパケットは、パケット中継手段 1 0 0 1 に送られる。

【 0 0 5 9 】

フィルタリング変更指示処理手段 1 0 0 9 は、認証サーバ 1 3 1 1 とネットワークを介して通信し、認証サーバ 1 3 1 1 からフィルタリング変更指示を受ける。本実施の形態では、通信プロトコルとして `telnet` を想定するが、HTTP や COPS (Common Open Policy Service) などのプロトコルを使用してもよい。フィルタリング変更指示は、対象とするエントリの内容と、追加／削除の指示を保持している。フィルタリング変更指示処理手段 1 0 0 9 は、送信元アドレス条件の IP アドレスが属するサブネットに接続された物理インターフェース 1 0 0 2 ～ 1 0 0 7 に対応するフィルタリング処理部 1 0 1 2 ～ 1 0 1 7 のフィルタリングテーブル 1 1 0 1 にその指示を反映させる。

【 0 0 6 0 】

図 1 3 は、本発明に関するルータ 1 0 0 0 を用いたネットワークの構成図である。

このネットワークは、例えば、ルータ 1 0 0 0 の各物理インターフェース 1 0 0 2 ～ 1 0 0 7 はそれぞれ接続されているサブネット A 1 3 0 2 ～ F 1 3 0 7 と、サブネット A 1 3 0 2 に接続されている認証サーバ 1 3 1 1 と、サブネット B 1 3 0 3 に接続されているファイルサーバ 1 3 2 2 と、サブネット C 1 3 0 4 ～ F 1 3 0 7 にそれぞれ接続され、ユーザが自由に端末を接続できる複数の情報コンセント 4 0 9 と、情報コンセント 4 0 1 を介してサブネット C 1 3 0 4 に接続されているユーザ端末 1 3 3 3 とを備えている。

【 0 0 6 1 】

各フィルタリングテーブル 1 1 0 1 の初期状態での内容は、フィルタリング処

理部A1012、B1013では何も登録されておらず、フィルタリング処理部C1014～F1017では、上述の図12の内容が設定されているものとする。

【0062】

つぎに、このネットワークで、ユーザ端末1333をサブネットC1304の情報コンセント409に接続した場合について説明する。

図14は、ユーザ端末1333を情報コンセント409に接続した際の通信シーケンス図である。

認証を受けていないユーザ端末1333が、ファイルサーバ1322にアクセスするためにファイルサーバ1322のIPアドレス(192.168.2.2)宛のファイルサーバ宛パケット1401を送信した場合、パケット1401は、ルータ1000の物理インターフェースC1004を介して、フィルタリング処理部C1014に送られる。フィルタリング処理部C1014のフィルタリングテーブル1101のうちパケット1401に該当するエントリは、#2のエントリであるので、パケット1401を廃棄する。したがって、ユーザ端末1333の送信するパケット1401は、ファイルサーバ1322に到達することはない。

【0063】

つぎに、ユーザ端末1333が認証を受けてファイルサーバ1322にアクセスする場合の動作を説明する。

ユーザ端末1333は、認証を受けるために認証サーバ1311のIPアドレス(192.168.1.1)宛のパケット1402を送信する。ルータ1000の物理インターフェースC1004からフィルタリング処理部C1014に送られたパケット1402に対して、フィルタリングテーブル1101の検索が行われる。この場合、フィルタリングテーブル1101のエントリ#1、#2の両方が該当するので、テーブル内で先に登録されている#1が適用される。このため、パケット1402は、パケット中継手段1001に送られる。

【0064】

したがって、ユーザ端末1333から認証サーバ1311への通信が成立する

。認証サーバ1311からユーザ端末1333への応答パケット1403は、物理インターフェースA1002からフィルタリング手段A1012に送られる。フィルタリング手段A1012のフィルタリングテーブル1101には何も登録されていないため、パケット1403は中継される。このため、ユーザ端末1333と認証サーバ1311との双方向の通信が成立することになり、ユーザ端末1333は、認証を受けることができる。

【0065】

認証サーバ1311は、ユーザ端末1333から送られてきたユーザIDとパスワード1404がネットワーク接続を許可されたユーザのものと一致した場合、ルータ1000のフィルタリング変更指示処理手段1009と通信すると共に、フィルタリングテーブル1101に、宛先アドレス条件が「任意」、送信元アドレス条件がユーザ端末1333のアドレスである「192.168.3.3」、中継／廃棄フラグが「中継」であるエントリを追加することを、ルータ1000に対して指示1405する。

【0066】

図15は、フィルタリングテーブル1101の構成図(2)である。

変更指示処理手段1009は、送信元アドレス条件「192.168.3.3」が属するサブネット(サブネットC1304)が物理インターフェースC1004に接続されているので、フィルタリング手段1314のフィルタリングテーブル1101に対して、エントリを追加する。その結果、フィルタリング手段C1014のフィルタリングテーブル1101には、エントリ#1～#3までが登録されていることになる。

【0067】

この状態で、ユーザ端末1333がファイルサーバ宛パケット1406を送信すると、フィルタリング手段C1014のフィルタリングテーブル1101のエントリ#1が該当するため、パケット1406は中継されることになり、ファイルサーバ1322へのアクセスが可能となる。

【0068】

以上のように、本実施の形態のルータ1000を用いることで、認証前のユー

ザ端末1333からファイルサーバ1322へのアクセスが阻止され、認証後はアクセスが可能になるネットワークを構築することができる。また、本実施の形態では、ルータ1000のネットワークインターフェースで複数の情報コンセント409を扱うことができ、さらに、ネットワークインターフェースごとに個別のフィルタリング手段を設けることにより、フィルタリング処理の負荷を分散することができる。

【0069】

(第3の実施の形態)

図16は、本発明に関するネットワーク間接続装置の第3の実施の形態の構成図である。

LANスイッチ1600は、例えば、パケット中継手段1601、複数のネットワークインターフェース1602～1605、アドレス学習テーブル1606、フィルタリングテーブル1607及び状態変更指示パケット処理手段1608を備える。ネットワークインターフェース1602～1605には、各々を一意に識別するために名前（図ではA～D）が割り当てられている。なお、名前は、一意に識別できれば番号等を用いてもよい。

【0070】

これらのネットワークインターフェース1602～1605は、それぞれ異なるネットワークに接続されており、パケットの送受信を行う。なお、本実施の形態でのネットワークは、IEEEの802.3ネットワークを用いるようにした。また、以下の本実施の形態を説明では、ネットワークインターフェースA1602を「アップリンク」、ネットワークインターフェースB1603～D1605を「ダウンリンク」と称する。

【0071】

パケット中継手段1601は、アドレス学習テーブル1606とフィルタリングテーブル1607の情報に基づいて、ネットワーク間でのパケット中継を行う。状態変更指示パケット処理手段1608は、後述する認証サーバ1901からの状態変更指示パケットを受信すると共に、フィルタリングテーブル1607と学習テーブル1606の内容を変更する。状態変更指示パケットには、IPアド

レスと「許可／禁止」が情報として保持されている。

【0072】

図17は、フィルタリングテーブル1607の構成図である。

フィルタリングテーブル1607には、中継を許可していないパケットを識別するための情報が登録されている。フィルタリングテーブル1607の各エントリは、MACアドレスフィールド1701、IPアドレスフィールド1702、接続ポートフィールド1703を含む。MACアドレスフィールド1701には、フィルタリング対象となるMACアドレスが、IPアドレスフィールド1702には、そのMACアドレスに対応するIPアドレスが、接続ポートフィールド1703には、そのMACアドレスを持つ端末が属するネットワークが接続されているネットワークインターフェース1602～1605の名前が、それぞれ登録されている。

【0073】

図18は、学習テーブル1606の構成図(1)である。

学習テーブル1606には、パケットの中継先ネットワークインターフェースに関する情報が登録されている。学習テーブル1606の各エントリは、MACアドレスフィールド1801及び接続ポートフィールド1802を含む。MACアドレスフィールド1801には、中継対象のMACアドレスが、接続ポートフィールド1802には、宛先MACアドレスがMACアドレスフィールドに一致したパケットを中継すべきネットワークインターフェース1602～1605の名前が、それぞれ登録されている。また、一定時間利用されなかったエントリは、自動的に学習テーブル1606から削除されるように設定されている。なお、本実施の形態では、ネットワーク間接続装置としてLANスイッチ1600を使用しているが、ルータ等その他のネットワーク間接続装置に対しても、本発明は適用可能である。

【0074】

次に、図19のネットワークを例に、本発明に関するLANスイッチ1600を用いたネットワークの動作を説明する。

図19は、本発明に関するLANスイッチ1600を用いたネットワークの構

成図である。

このネットワークは、例えば、LANスイッチ1600と、LANスイッチ1600の各ネットワークインターフェース1602～1605にそれぞれ接続されたネットワークA～Dと、ネットワークB～Dを介して、ダウンリンクの各ネットワークインターフェースB1603～D1605に接続された、ユーザが自由に端末を接続できる複数の情報コンセント409と、情報コンセント409を介してネットワークBに接続されたユーザ端末1905と、アップリンクのネットワークAに接続されたルータ1904と、ネットワークを介してルータ1904に接続された、ファイルサーバ1902、DHCPサーバ1903、認証サーバ1901とを備える。

【0075】

ルータ1904は、BOOTPリレーエージェント機能を備えると共に、IPプロトコルに基づいた中継を行う。DHCPサーバ1903は、DHCPプロトコルに基づきユーザ端末にIPアドレスを配布する。認証サーバ1901は、ユーザ認証の結果を状態変更指示パケットにしてLANスイッチ1600に通知する。

【0076】

つぎに、初期状態で、ユーザ端末1905をネットワークBの情報コンセント409に接続した場合について説明する。

図20は、ユーザ端末1905をネットワークBの情報コンセント409に接続した際の通信シーケンス図である。

初期状態では、LANスイッチ1600のフィルタリングテーブル1607には、何も登録されていない。また、学習テーブル1606のMACアドレス1801には、ルータ1904のMACアドレス(22:22:00:44:44:44)が、同じく接続ポート1802には、ネットワークインターフェースA1602が、それぞれ登録されている。

【0077】

まず、ユーザ端末1905は、情報コンセント409に接続されると、DHCPプロトコルによりIPアドレスを要求するためのアドレス要求パケット200

1を、ブロードキャストアドレス宛に送信する。ここで、パケット2001を受信したLANスイッチ1600の中継処理を説明する。

【0078】

図21は、パケット受信に対するLANスイッチ1600の中継処理を示すフローチャートである。

ここでは、パケット2001の宛先アドレスは、学習テーブル1606に登録なしであり（処理2101）、かつ、ブロードキャストアドレスである（処理2102）。また、受信ポートはネットワークインターフェースB1603で、アップリンクではない（処理2103）。さらに、送信元MACアドレスが学習テーブル1606にない（処理2104）。また、フィルタリングテーブル1607に送信元MACアドレスがないことから、ユーザ端末1905のアドレス（22:22:FF:00:00:01）をフィルタリングテーブル1607に登録する（処理2105）。

【0079】

ここで、フィルタリングテーブル1607では、図17に示すように、IPアドレス1702に「未登録」、接続ポート1703に「B」がそれぞれ登録される。これにより、パケット2001は、アップリンクにのみ中継され、ルータ1904に送られる（処理2105）。

ここで、再び通信シーケンスの説明をする。パケット2001は、DHCPパケットであるので、ルータ1904のBOOTPリレーエージェント機能により、DHCPサーバ1903に中継される。DHCPサーバ1903からのアドレス配布パケット2002は、ルータ1904のBOOTPリレーエージェント機能により、ユーザ端末1905のMACアドレス（22:22:FF:00:00:01）宛に送られる。

【0080】

LANスイッチ1600は、パケット2002を中継処理する。ここで、上述のフローチャートの説明に戻る。パケット2002は、宛先MACアドレスが学習テーブル1607になく（処理2101）、かつ、宛先がブロードキャストではない（処理2102）。また、フィルタリングテーブル1607に宛先があり

(処理2106)、かつ、受信ポートがネットワークインターフェースA1602であり、アップリンクである(処理2107)。さらに、プロトコルがIPであり(処理2108)、送信元IPアドレスがリレーエージェント(ルータ1904)のIPアドレスである(処理2109)。

【0081】

フィルタリングテーブル1607のエントリ#1により、接続ポート1703がネットワークインターフェースB1603であることがわかるので、パケット2002をネットワークインターフェースB1603から送信する(処理2110)。これにより、ユーザ端末1905にアドレス配布パケット2002が送られることになる。ここで、ユーザ端末1905に、DHCPサーバ1903から配布されたアドレスを「192.168.5.1」とする。

【0082】

ここで、ユーザ端末1905が認証を受けずにファイルサーバ1902にアクセスを試みる場合について説明する。但し、アクセスのためのプロトコルはIPを用いる。

まず、ファイルサーバ1902(アドレス192.168.1.2)とユーザ端末1905(アドレス192.168.5.1)ではIPサブネットが異なるので、ファイルサーバ1902にアクセスするためのパケット2003は、宛先IPアドレスがファイルサーバ1902の(192.168.1.2)で、宛先MACアドレスがルータ1904の(22:22:00:44:44:44)である。

【0083】

ここで、ファイルアクセスパケット2003を受信したLANスイッチ1600の処理を説明する。

まず、宛先MACアドレスが学習テーブル1606に登録されている(処理2101)。送信元MACアドレスがフィルタリングテーブル1607に登録されており、送信元IPアドレスであって、DHCPサーバ1903からユーザ端末1905に配布されたIPアドレス(192.168.5.1)を「未登録」であったIPアドレスフィールド1702に登録する(処理2111)。これによ

り、パケット2003は、IPの仕様に基づいて中継されることになり、ルータ1904を経由して、ファイルサーバ1902に送信されると共に、ファイルサーバ1902からの応答としてデータパケット2004が送られる。

【0084】

ここで、パケット2004を受信したLANスイッチ1600の処理について説明する。

ルータ1904を経由してLANスイッチ1600に送られたパケット2004は、宛先MACアドレスが学習テーブル1606になく（処理2101）、かつ、宛先がブロードキャストでもない（処理2102）。また、フィルタリングテーブル1607に登録があり（処理2106）、かつ、受信ポートがネットワークインターフェースAであり、アップリンクである（処理2107）。さらに、プロトコルがIP（処理2108）であり、送信元IPアドレスがファイルサーバのアドレスなので廃棄される（処理2109）。したがって、パケット2004は、ユーザ端末1905に届かないため、アクセスは成立しない。

【0085】

つぎに、ユーザ端末1905が認証を行う場合について説明する。

まず、ユーザ端末1905からユーザIDとパスワードパケット2005が認証サーバ1901に送られる。認証サーバ（アドレス192.168.1.1）とユーザ端末1905（アドレス192.168.5.1）では属するサブネットワークが異なるので、パケット2005の宛先IPアドレスは、認証サーバ1901のIPアドレスであり、宛先MACアドレスは、ルータ1904のMACアドレスとなる。

【0086】

ここで、パケット2005を受信したLANスイッチ1600の処理について説明する。LANスイッチ1600では、宛先MACアドレスが学習テーブル1606に登録済みであるので（処理2101）、パケット2005を認証サーバ1901に中継する。

【0087】

認証サーバ1901では、ユーザ端末1905から送られたユーザIDとパス

ワードがネットワークの使用を許可されたユーザのものであった場合、状態変更指示通知パケット2006をLANスイッチ1600の状態変更指示通知パケット処理手段1609に送信する。このパケット2006には、IPアドレス(192.168.5.1)と「許可」が情報として含まれる。この状態変更指示通知パケット2006を受けた状態変更指示通知パケット処理手段1609は、フィルタリングテーブル1607からIPアドレス(192.168.5.1)を検索する。

【0088】

図22は、学習テーブル1606の構成図(2)である。

フィルタリングテーブル1607からIPアドレス(192.168.5.1)を検索することで得られたMACアドレスフィールド1701と接続ポートフィールド1703とを、新たなエントリとして、学習テーブル1606に追加する。

【0089】

ここで、ユーザ端末1905がファイルサーバ1902へのアクセスを試みると、上述のように、このファイルアクセスパケット2007は、ファイルサーバ1902に届く。その応答データであるパケット2008は、LANスイッチ1600で次のように処理される。

【0090】

パケット2008の宛先MACアドレスは、ユーザ端末1905のMACアドレス(22;22:FF:00:00:01)であるので、現在の学習テーブル1606(図22)に登録されている(処理2101)。したがって、処理2111を経て、パケット2008は中継され、ユーザ端末1905に届く。これにより、今回はファイルサーバ1902へのアクセスが成立する。

【0091】

また、ユーザ端末1905が一定時間通信をしなかった場合、学習テーブル1606のエントリが自動的に削除されるので、再び認証を行うまではファイルサーバ1902へのアクセスはできなくなる。また、DHCPによるアドレス配布では、通常、配布したアドレスの使用期限を設けている。このため、DHCPサ

サーバ1903は、アドレス配布2002を行ってから時間が経過し使用期限が過ぎたら、タイムアウト通知2009を認証サーバ1901に対して行う。タイムアウト通知2009を受けた認証サーバは、IPアドレスとしてタイムアウトしたアドレス（この場合192.168.5.1）、および「禁止」という情報を含む状態変更指示通知パケット2010をLANスイッチ1600の状態変更指示通知パケット処理手段1609に送信する。

【0092】

状態変更指示通知パケット処理手段1609は、IPアドレス（192.168.5.1）をフィルタリングテーブル1607から検索し、対応するMACアドレスフィールド1701に登録されたMACアドレス（この場合22:22:FF:00:00:01）を、学習テーブル1606から検索する。そして、フィルタリングテーブル1607と学習テーブル1606の双方から該当するエントリを削除する。その結果、ユーザ端末1905は、再び認証を受けなければファイルサーバ1902にアクセスできなくなる。

【0093】

以上のように、本実施の形態のLANスイッチ1600を用いることで、認証を受けていないユーザ端末1905からのファイルサーバ1902へのアクセスを防止すると共に、認証を受けたユーザ端末1905からのファイルサーバ1902へのアクセスを許可するネットワークを構築できる。また、本実施の形態では、一定時間無通信である場合や、アドレスの有効期限が切れた場合に、LANスイッチのテーブルを自動的に変更し、再び認証を受けるまではファイルサーバ1902へのアクセスを防止することもできる。

【0094】

（第4の実施の形態）

図23は、本発明に関するルータ2300を用いたネットワークの構成図である。

ルータ2300は、本発明に関するネットワーク間接続装置の第4の実施の形態であり、例えば、複数のネットワークインターフェース2302～2305、パケット中継手段2301、IPアドレス登録表2306を備える。

【 0 0 9 5 】

パケット中継手段 2 3 0 1 は、 I P プロトコルに基づいてパケット中継を行い、 I P アドレス登録表 2 3 0 6 に登録されていないアドレスからのパケットに対して、カプセル化処理を行う。ネットワークインターフェース A 2 3 0 2 ~ D 2 3 0 5 は、それぞれ異なるネットワークに接続され、パケットの送受信を行う。 I P アドレス登録表 2 3 0 6 には、認証を受けたユーザ端末の I P アドレスが登録される。

【 0 0 9 6 】

また、このネットワークは、例えば、ルータ 2 3 0 0 と、ルータ 2 3 0 0 のネットワークインターフェース A 2 3 0 2 に、ネットワーク A を介して接続された認証サーバ 2 3 1 0 及びファイルサーバ 2 3 1 1 と、ネットワークインターフェース B 2 3 0 3 ~ D 2 3 0 5 に、ネットワーク B ~ D を介して接続され、ユーザが端末を自由に接続できる複数の情報コンセント 4 0 9 と、情報コンセント 4 0 9 を介してネットワーク B 2 3 0 3 に接続されたユーザ端末 2 3 1 2 とを備える。認証サーバ 2 3 1 0 は、ユーザ認証を行うと共に、その結果をルータ 2 3 0 0 に通知し、後述するカプセル化したパケットの送受信を行う。

【 0 0 9 7 】

つぎに、初期状態で、ユーザ端末 2 3 1 2 をネットワーク B 2 3 1 3 に接続した場合について説明する。ここで、図 2 7 は、初期状態での I P アドレス登録表 2 3 0 6 の構成図である。

図 2 4 は、ユーザ端末 2 3 1 2 をネットワーク B 2 3 1 3 に接続した際の通信シーケンス図である。

まず、ユーザ端末 2 3 1 2 が認証を受けずにファイルアクセスを試みた場合について説明する。

ルータ 2 3 0 0 は、ユーザ端末 2 3 1 2 からのファイルアクセスパケット 2 4 0 0 を受信すると共に、このパケット 2 4 0 0 に対して中継処理を行う。

【 0 0 9 8 】

図 2 5 は、パケット受信に対するルータ 2 3 0 0 の中継処理を示すフローチャートである。

パケット2400の宛先アドレスは、ファイルサーバ2311のアドレスであり、ルータのカプセル化アドレスではない（処理2501）。また、送信元アドレスは、IPアドレス登録表2306に登録されていないので（処理2502）、パケット2400は、カプセル化される（処理2503）。

【0099】

ここで、「カプセル化」とは、IPヘッダを含むパケット2400全体をデータとみなし、このデータに対して、宛先アドレスを認証サーバ2310のカプセル化アドレス（192.168.100.100）、送信元アドレスをルータ2300のカプセル化アドレス（192.168.100.101）とするIPヘッダを付加することで、新たなパケット（カプセル化したパケット）を作成することである。このため、カプセル化したパケットは、元々の宛先アドレス（例えば、ファイルサーバ2311のアドレス）に係わらず、認証サーバ2310に送信されることになる（処理2504）。

【0100】

ここで、カプセル化されたパケットを受信した認証サーバ2310の処理について説明する。

図26は、パケット受信に対する認証サーバ2310の処理を示すフローチャートである。

カプセル化されたパケットの宛先アドレスは、認証サーバのカプセル化アドレスであり（処理2601）、かつ、送信元アドレスは、ルータのカプセル化アドレスである（処理2602）。したがって、パケット2400のカプセル化を解除し、元々のパケット2400を復元する（処理2603）。元々のパケット2400の宛先アドレスは、ファイルサーバ2311のアドレスであって、認証サーバ2310のアドレスではないので（処理2604）、パケットは廃棄される。したがって、認証前のユーザ端末2312は、ファイルサーバ2311へアクセスすることはできない。

【0101】

つぎに、ユーザ端末2312が認証を受けるためユーザIDとパスワードを含むパケット2401を認証サーバ2310のアドレス宛に送った場合について、

図 24 及び 25 を用いて説明する。

パケット 2400 を受信したルータ 2300 では、パケット 2401 の宛先アドレスがルータのカプセル化アドレスではなく（処理 2501）、かつ、送信元アドレスが IP アドレス登録表 2306 に登録されていない（処理 2502）。このため、パケット 2401 は、カプセル化されると共に（処理 2503）、認証サーバ 2310 に送信される（処理 2504）。

【0102】

また、認証サーバ 2310 では、宛先アドレスが認証サーバのカプセル化アドレスであり（処理 2601）、送信元アドレスがルータ 2300 のカプセル化アドレスである（処理 2602）。このため、パケット 2401 のカプセル化を解除する（処理 2603）。ここで、元々のパケット 2401 の宛先アドレスは、認証サーバ 2310 のアドレスであるので（処理 2604）、認証を行う（処理 2605）。さらに、送られてきたパケット 2401 に含まれるユーザ ID とパスワードがネットワークの使用許可を与えられたユーザのものと一致したら、認証成功を通知するパケット 2402 をカプセル化して送信する（処理 2606）。この認証サーバ 2310 でのカプセル化は、宛先アドレスをルータ 2300 のカプセル化アドレス（192.168.100.101）とし、送信元アドレスを認証サーバ 2310 のカプセル化アドレス（192.168.100.100）とする。

【0103】

さらに、ルータ 2300 では、カプセル化された認証成功の通知パケット 2402 を受信し、宛先アドレスがルータのカプセル化アドレスであり（処理 2501）、かつ、送信元アドレスは認証サーバのカプセル化アドレスである（処理 2505）。このため、パケット 2402 のカプセル化を解除すると共に（処理 2506）、復元したパケット 2402 を中継する（処理 2507）。

【0104】

また、認証サーバ 2310 では、ユーザ端末 2312 の認証が成功すると、ルータ 2300 に対して、IP アドレス（192.168.3.3）の登録を指示する IP アドレス登録パケット 2403 を送信する。その結果、IP アドレス登

録表2306にIPアドレス(192.168.3.3)が登録される。

【0105】

つぎに、ユーザ端末2312がファイルサーバ2311にアクセスするためのファイルアクセスパケット2404を送信する場合について説明する。パケット2404の宛先アドレスがルータのカプセル化アドレスではなく(処理2501)、送信元アドレスであるユーザ端末2312のIPアドレス(192.168.3.3)がIPアドレス登録表2306に登録されている(処理2502)。このため、パケット2404は、ファイルサーバ2311に中継される(処理2508)。

【0106】

同様に、ファイルサーバ2311からの応答データであるパケット2405は、ファイルサーバ2311のアドレス(192.168.10.2)がIPアドレス登録表2306に登録されているので、ユーザ端末2312に中継される。したがって、認証を受けた後は、ユーザ端末2312からファイルサーバ2311へのアクセスが可能となる。

【0107】

さらに、認証サーバ2310は、ユーザ認証が成功した後、定期的にユーザ端末2312に対してICMP(Internet Control Message Protocol)のICMPエコーリクエスト2406を送信し、ユーザ端末2312から応答データであるICMPエコーリプライ2407が返ってくることを確認する。

【0108】

ICMPエコーリクエスト2406を送信してから一定時間以内にユーザ端末2312からの応答がない場合、認証サーバ2310は、ユーザ端末2312のIPアドレス(192.168.3.3)をIPアドレス登録表から削除する指示をルータ2300に送信する。その結果、ユーザ端末2312のアドレスは、IPアドレス登録表2306から削除され、再び認証を受けるまでは、ユーザ端末2312からファイルサーバ2311へのアクセスはできなくなる。

【0109】

以上のように、本実施の形態のルータ2300を用いることで、認証を受けて

いないユーザ端末 2 3 1 2 からファイルサーバ 2 3 1 1 へのアクセスを防止すると共に、認証を受けたユーザ端末 2 3 1 2 からのファイルサーバ 2 3 1 1 へのアクセスを許可するネットワークシステムを構築することができる。また、本実施の形態では、定期的にユーザ端末 2 3 1 1 からの応答を確認することにより、ユーザ端末 2 3 1 1 がネットワークから離脱したり、使用を中止した場合、ファイルサーバ 2 3 1 1 へのアクセス許可を自動的に取り消すことができる。

【 0 1 1 0 】

【発明の効果】

本発明によると、以上説明した通り、ユーザが任意の時刻及び場所に端末を接続しても、認証を受けたユーザにのみネットワーク上の資源へのアクセスを許可すると共に、認証を受けていない不正なユーザからのネットワーク上の資源へのアクセスを禁止することができる。

【図面の簡単な説明】

【図 1】

本発明に関するネットワーク間接続装置の第 1 の実施の形態の構成図。

【図 2】

ネットワークインターフェース 1 0 2 ～ 1 0 7 の構成図。

【図 3】

アドレス学習テーブル 1 0 8 の構成図（1）。

【図 4】

本発明に関する LAN 1 0 0 を用いたネットワークの構成図。

【図 5】

ユーザ端末 4 0 3 を情報コンセント 4 0 9 に接続した際の通信シーケンス図。

【図 6】

パケット受信に対する LAN スイッチ 1 0 0 の中継処理を示すフローチャート

【図 7】

アドレス学習テーブル 1 0 8 の構成図（2）。

【図 8】

処理 6 0 4 のフローチャート。

【図 9】

中継テーブル 9 0 1 の構成図。

【図 1 0】

本発明に関するネットワーク間接続装置の第 2 の実施の形態の構成図。

【図 1 1】

フィルタリング処理部 1 0 1 2 ~ 1 0 1 7 の構成図。

【図 1 2】

フィルタリングテーブル 1 1 0 1 の構成図 (1) 。

【図 1 3】

本発明に関するルータ 1 0 0 0 を用いたネットワークの構成図。

【図 1 4】

ユーザ端末 1 3 3 3 を情報コンセント 4 0 9 に接続した際の通信シーケンス図

【図 1 5】

フィルタリングテーブル 1 1 0 1 の構成図 (2) 。

【図 1 6】

本発明に関するネットワーク間接続装置の第 3 の実施の形態の構成図。

【図 1 7】

フィルタリングテーブル 1 6 0 7 の構成図。

【図 1 8】

学習テーブル 1 6 0 6 の構成図 (1) 。

【図 1 9】

本発明に関する LAN スイッチ 1 6 0 0 を用いたネットワークの構成図。

【図 2 0】

ユーザ端末 1 9 0 5 をネットワーク B の情報コンセント 4 0 9 に接続した際の通信シーケンス図。

【図 2 1】

パケット受信に対する LAN スイッチ 1 6 0 0 の中継処理を示すフローチャー

ト。

【図 2 2】

学習テーブル 1 6 0 6 の構成図 (2) 。

【図 2 3】

本発明に関するルータ 2 3 0 0 を用いたネットワークの構成図。

【図 2 4】

ユーザ端末 2 3 1 2 をネットワーク B 2 3 1 3 に接続した際の通信シーケンス図。

【図 2 5】

パケット受信に対するルータ 2 3 0 0 の中継処理を示すフローチャート。

【図 2 6】

パケット受信に対する認証サーバ 2 3 1 0 の処理を示すフローチャート。

【図 2 7】

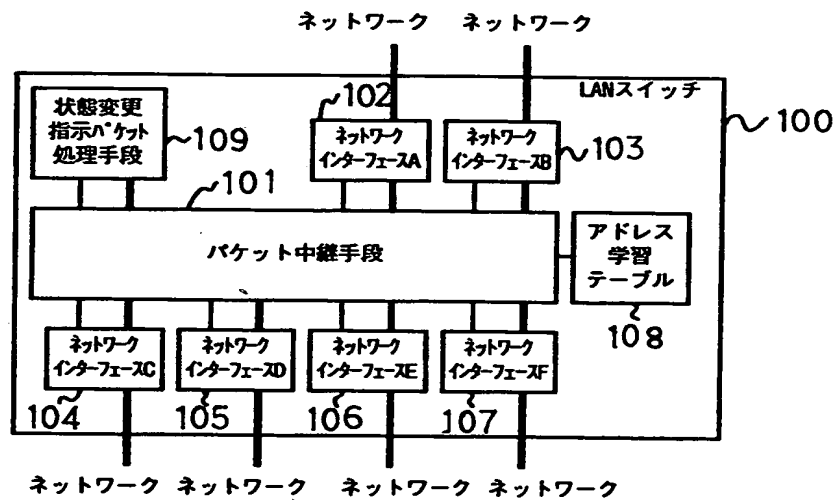
初期状態での I P アドレス登録表 2 3 0 6 の構成図。

【符号の説明】

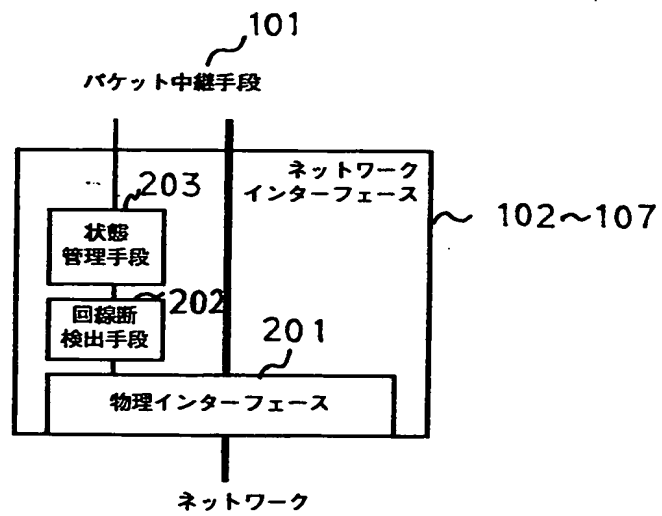
- 1 0 0 L A N スイッチ
- 1 0 9 状態変更指示パケット処理手段
- 2 0 3 状態管理手段
- 4 0 1 認証サーバ
- 4 0 2 ファイルサーバ
- 4 0 3 ユーザ端末
- 4 0 9 情報コンセント

【書類名】 図面

【図 1】



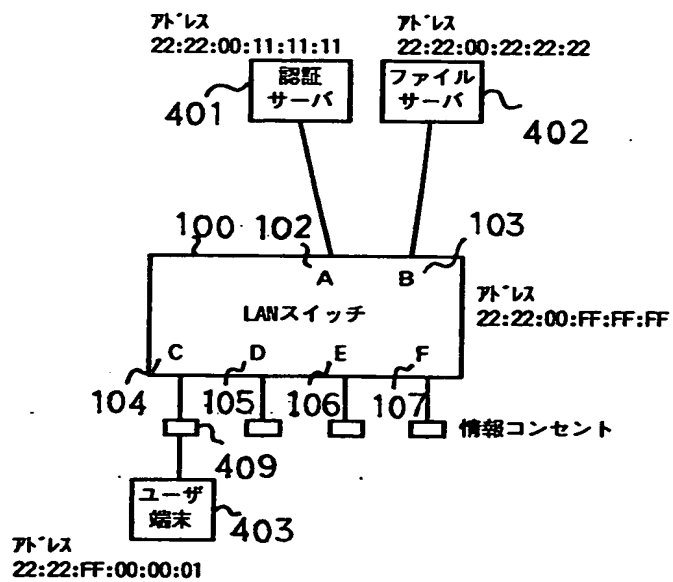
【図 2】



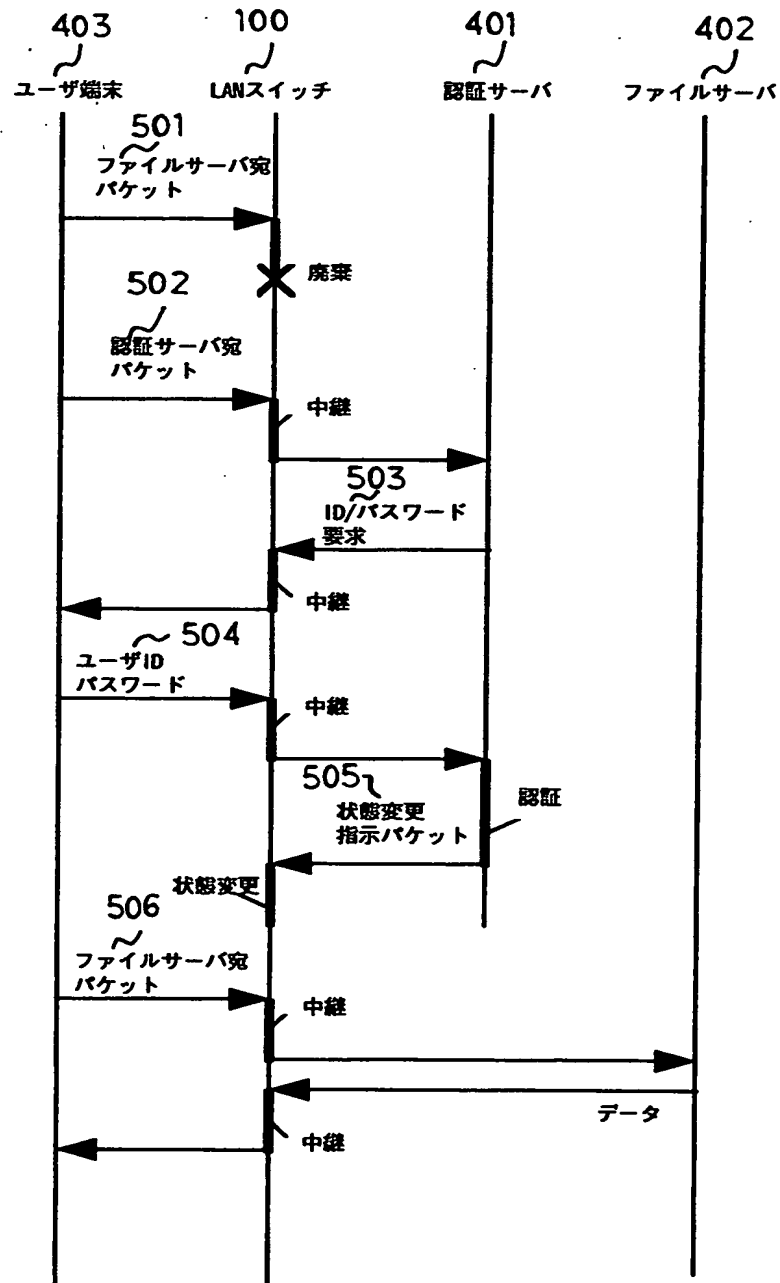
【図 3】

#	アドレス	送信ポート
1	22:22:00:11:11:11	A
2	22:22:00:22:22:22	B
3	22:22:00:FF:FF:FF	X

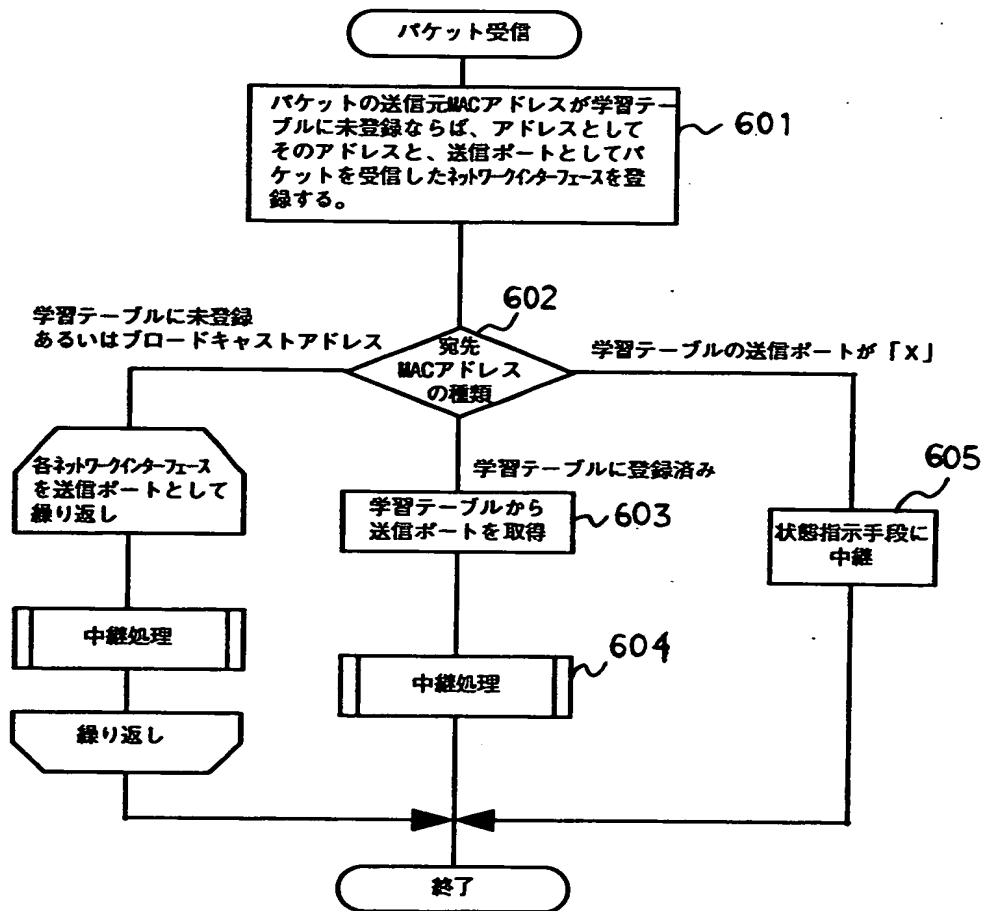
【図 4】



【図 5】



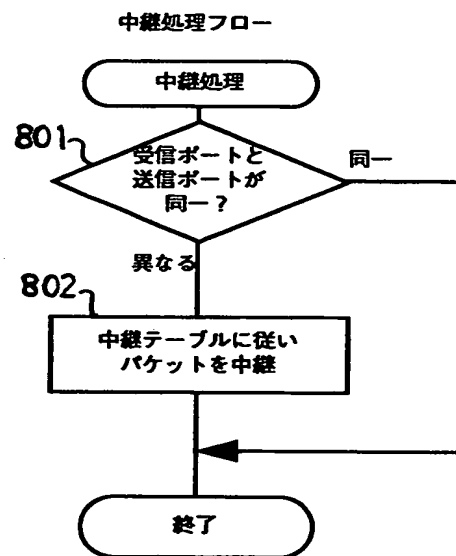
【図 6】



【図 7】

#	アドレス	送信ポート
1	22:22:00:11:11:11	A
2	22:22:00:22:22:22	B
3	22:22:00:FF:FF:FF	X
4	22:22:FF:00:00:01	C

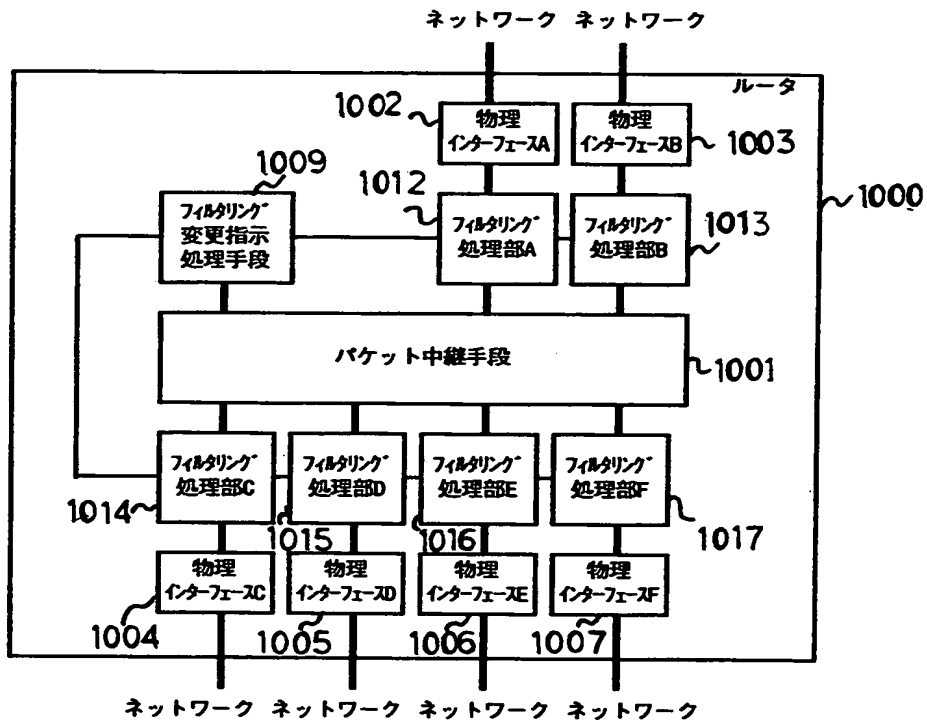
【図 8】



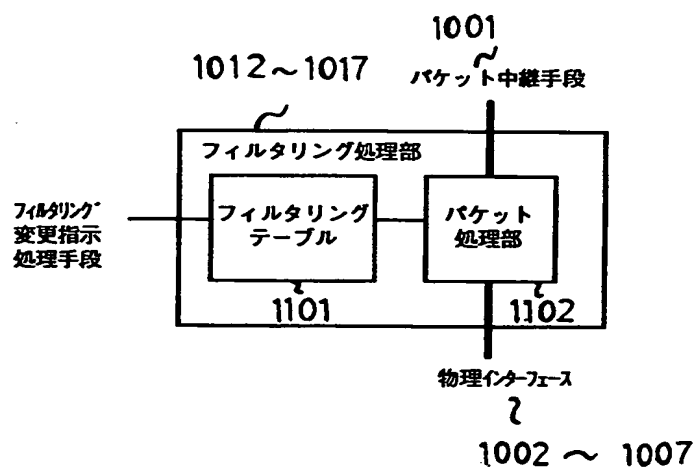
【図 9】

		受信ポートの状態		
		接続状態	非接続状態	状態なし
送信ポートの状態	接続状態	中継	廃棄	中継
	非接続状態	廃棄	廃棄	中継
	状態なし	中継	中継	中継

【図 10】



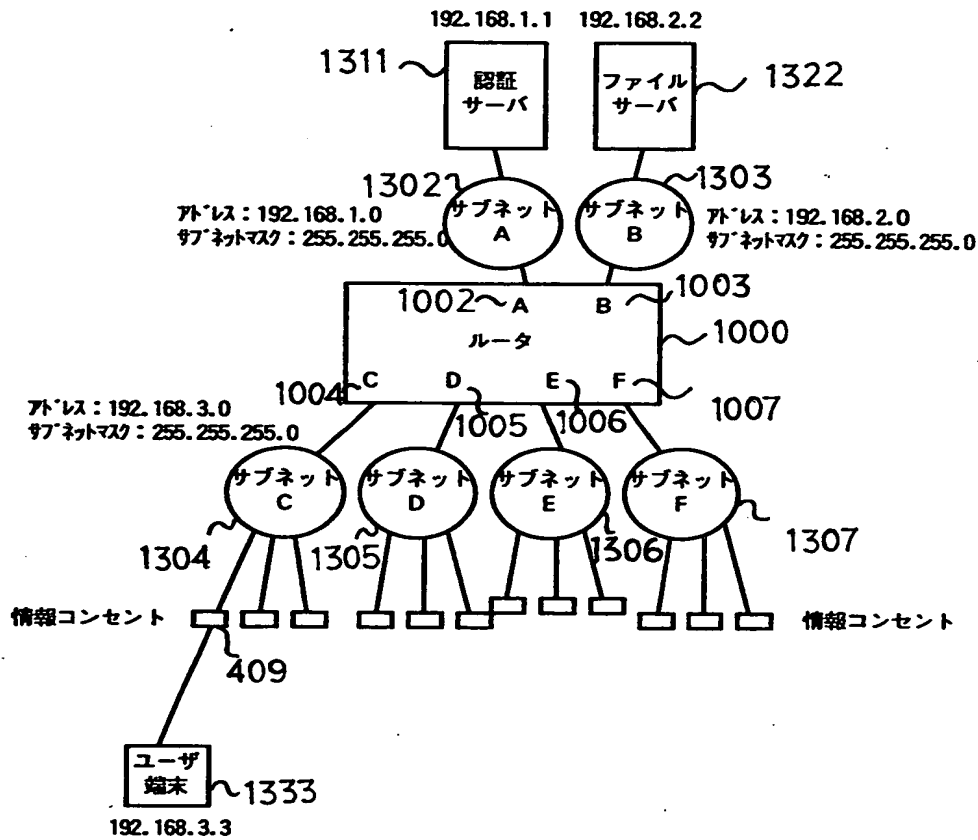
【図 1 1】



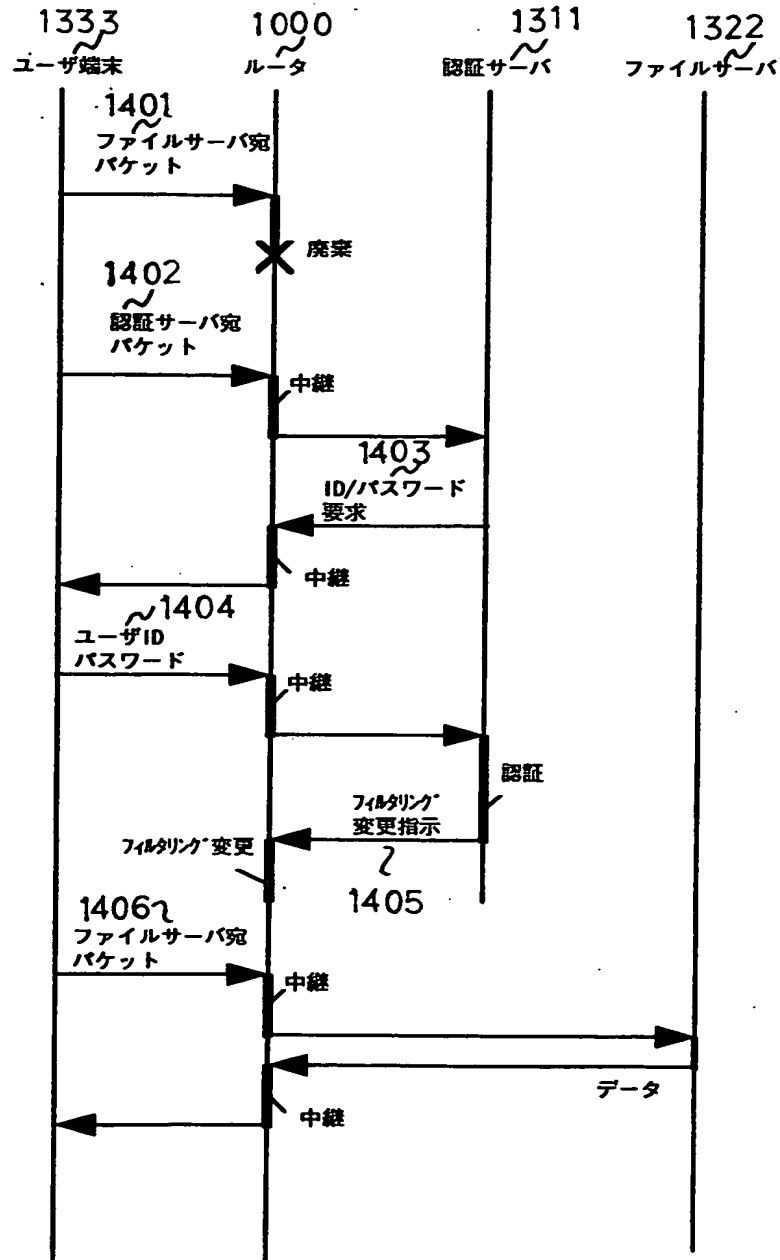
【図 1 2】

#	宛先アドレス条件	送信元アドレス条件	中継/廃棄フラグ
1	192.168.1.1	任意	中継
2	任意	任意	廃棄

【図 13】



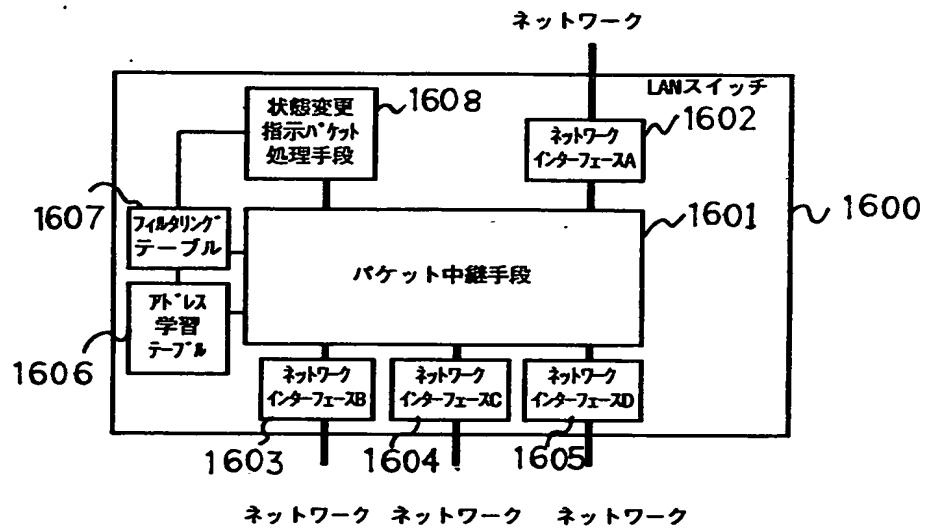
【図14】



【図 1 5】

#	宛先アドレス条件	送信元アドレス条件	中継／廃棄フラグ
1	任意	192.168.3.3	中継
2	192.168.1.1	任意	中継
3	任意	任意	廃棄

【図 1 6】



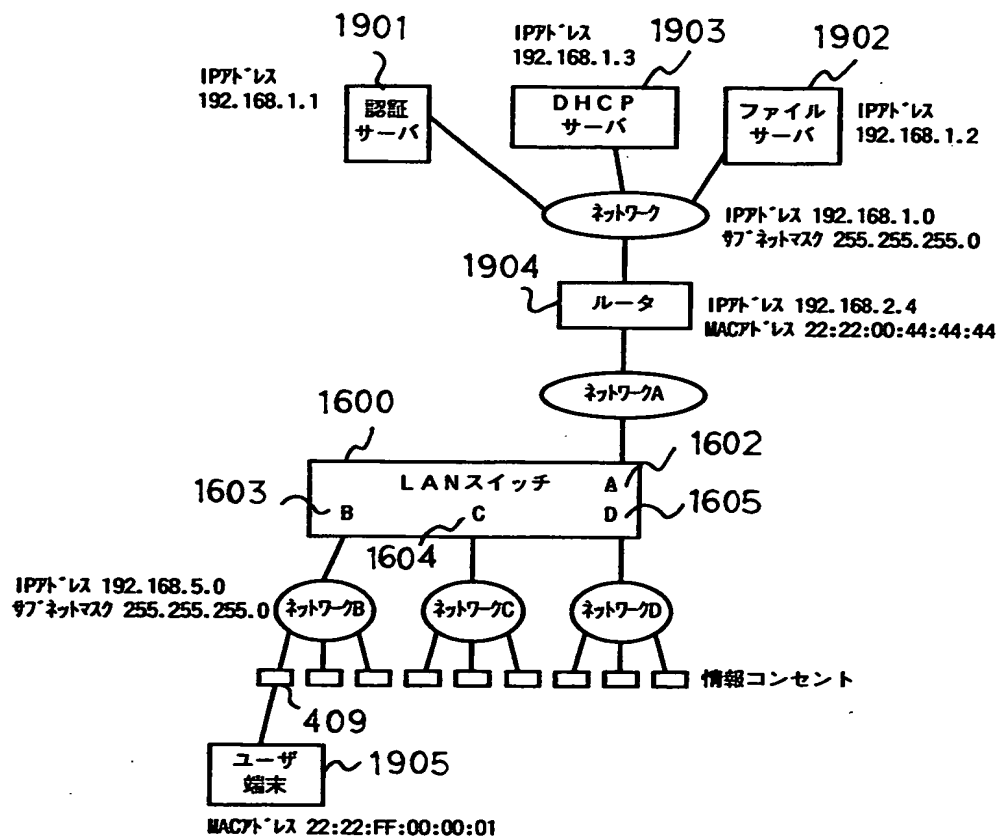
【図 17】

1607	1701	1702	1703
✓	✓	✓	✓
#	MAC アドレス	IP アドレス	接続ポート
1	22:22:FF:00:00:01	未登録	B

【図 18】

#	MAC アドレス	接続ポート
1	22:22:00:44:44:44	A

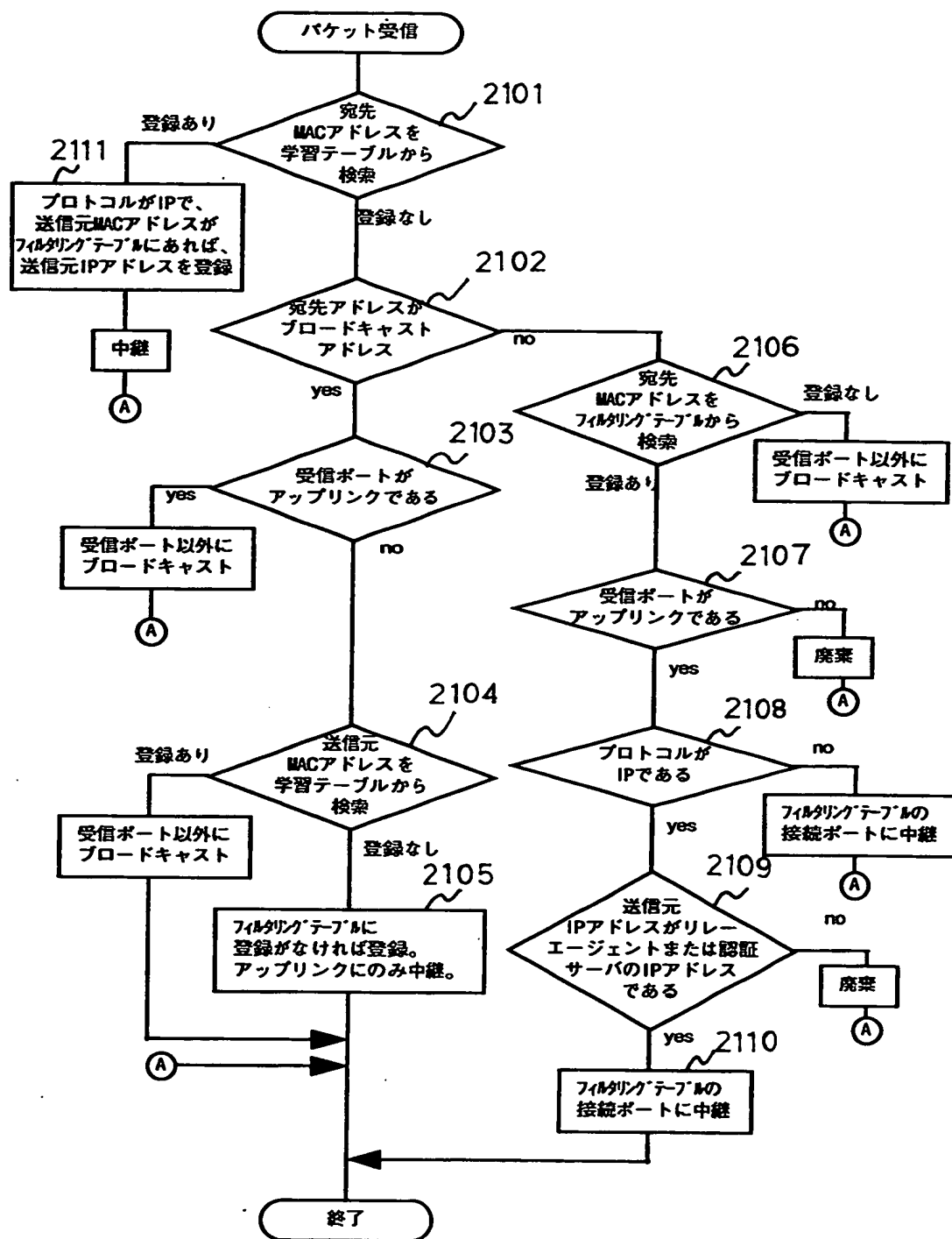
【図19】



【图 20】



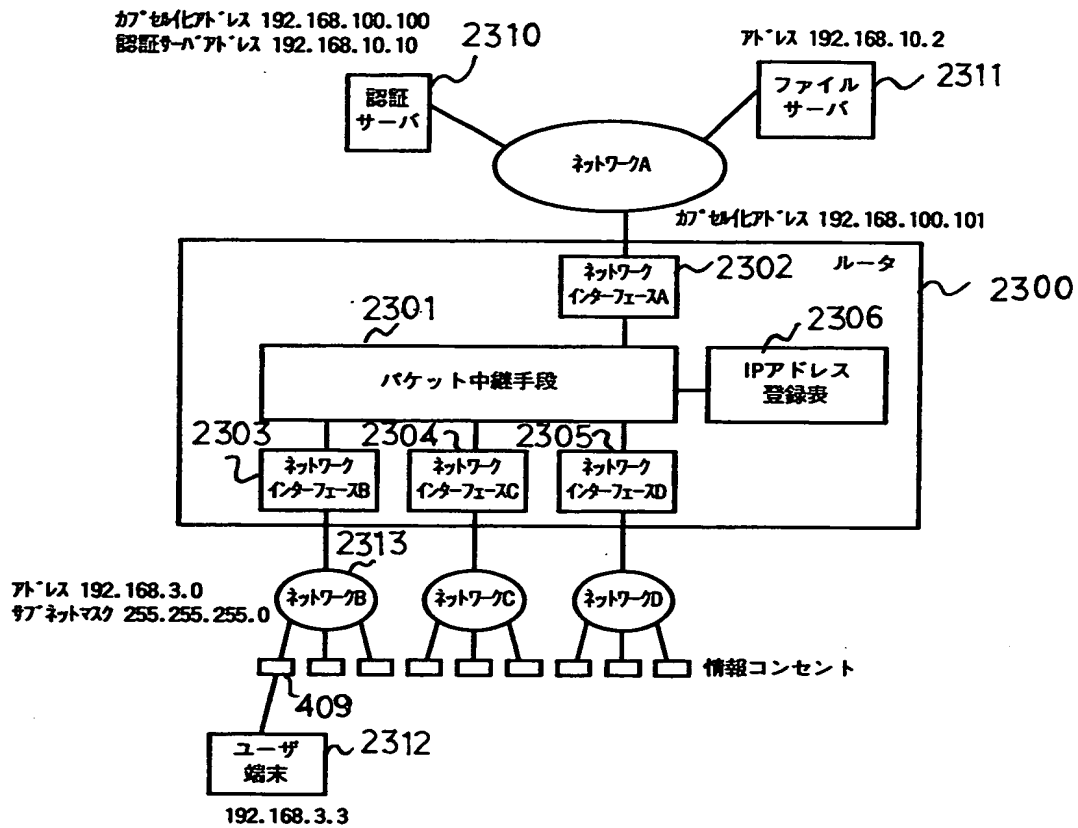
【図 21】



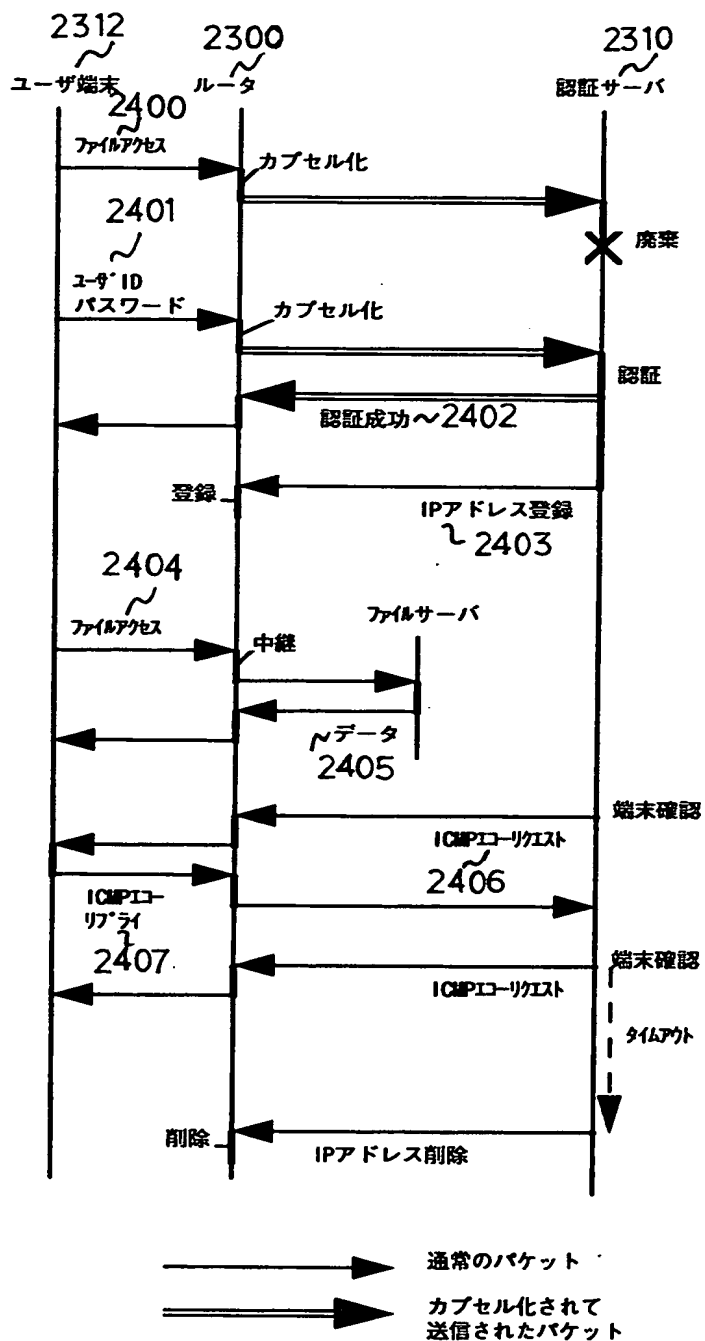
【図 22】

1606	1801	1802
#	MAC アドレス	接続ポート
1	22:22:00:44:44:44	A
2	22:22:FF:00:00:01	B

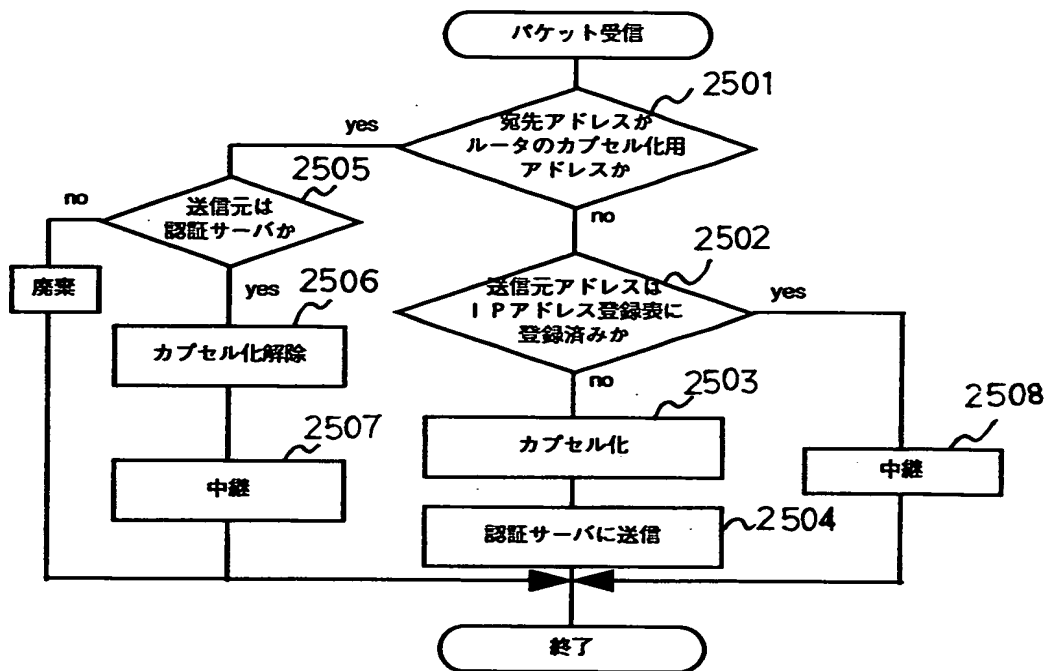
【図 23】



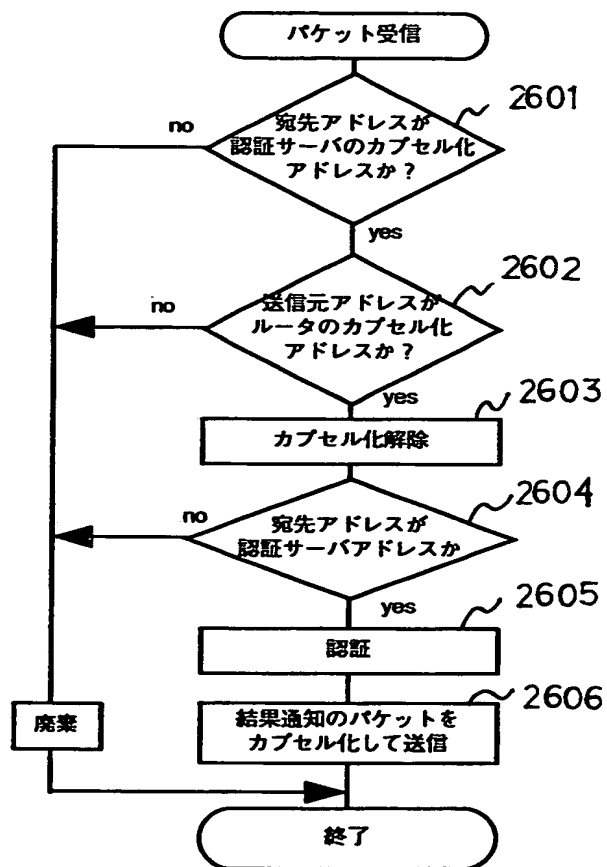
【図 2 4】



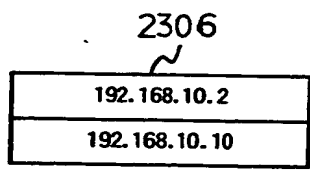
【図 2 5】



【図 26】



【図 2 7】



【書類名】 要約書

【要約】

【課題】 不正な利用者がネットワークを不正に利用することを防止する。

【解決手段】 LAN 1 0 0 は、パケット中継手段 1 0 1、複数のネットワークインターフェース 1 0 2 ～ 1 0 7、アドレス学習テーブル 1 0 8 及び状態変更指示パケット処理手段 1 0 9 を備え、状態変更指示パケット処理手段 1 0 9 は、特定のネットワークインターフェースの状態を「接続状態」、「非接続状態」及び「状態なし」のいずれかの状態に変更する指示を保持する状態変更指示パケットを、パケット中継手段 1 0 1 を介して認証サーバ 4 0 1 から受信すると共に、この状態変更指示パケットを、特定のネットワークインターフェース内の状態管理手段 2 0 3 に送信する。この状態管理手段 2 0 3 は、状態変更指示パケットに基づいて、特定のネットワークインターフェースの状態を「接続状態」、「非接続状態」及び「状態なし」のいずれかの状態に変更する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005108]

1. 変更年月日	1990年 8月31日
[変更理由]	新規登録
住 所	東京都千代田区神田駿河台4丁目6番地
氏 名	株式会社日立製作所